HOLLAND & KNIGHT LLP
Richard Williams (State Bar No. 52896)
633 West Fifth Street, 21st Floor
Los Angeles, California 90071-2040
Telephone (213) 896-2400
Facsimile (213) 896-2450

Attorneys for Plaintiff IneoQuest Technologies, Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

INEOQUEST TECHNOLOGIES, INC.

Plaintiff

vs.

IXIA

Defendant

JSL

Case No.: CV08-07773 PLAx

COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff, IneoQuest Technologies, Inc. (hereinafter referred to as "IneoQuest"), as and for its Complaint hereby pleads as follows:

Preliminary Statement

1. The plaintiff, IneoQuest Technologies, Inc. ("IneoQuest") brings this action against the defendant, Ixia ("Ixia"), seeking damages and injunctive relief for patent infringement, trade secret misappropriation, unfair competition, and other wrongs.

2. IneoQuest pioneered key developments in the fields of testing and monitoring the delivery of streaming video over packetized networks (such as the Internet), and created the industry-standard "MDI" measure for gauging the quality of a packetized video stream.

3. Although an established presence in other network-transport fields – namely data and voice -- Ixia had little experience or knowledge in video streaming. Rather than acquire this knowledge legitimately through licensing or independent development, Ixia misappropriated the knowledge from IneoQuest in breach of a written non-disclosure agreement. Ixia then employed a variety of wrongful strategies designed to block IneoQuest from the market, to put IneoQuest "out of business," and to interfere with and harm IneoQuest's key customer relationships. Ixia now infringes IneoQuest's core patent.

Parties

4. The plaintiff, IneoQuest Technologies, Inc. ("IneoQuest") is a corporation organized and existing under the laws of the Commonwealth of Massachusetts, with a principal place of business is located at 170 Forbes Blvd., Mansfield, Massachusetts 02048.

5. The defendant, Ixia ("Ixia"), is a corporation organized and existing under the laws of the State of California, with a principal place of business is located at 26601 W. Agoura Road, Calabasas, California 91302.

Jurisdiction And Venue

6. This is an action for patent infringement arising under the Patent Act, 35 U.S.C. § 1, et seq. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338.

7. This Court has supplemental jurisdiction over IneoQuest’s state, statutory, and common law claims under 28 U.S. C. § 1367(a), because these claims are so related to the federal claims in this action that they form part of the same case or controversy.

8. This Court has personal jurisdiction over the defendant in that the defendant is organized under the laws of the State of California, and has its principal place of business in California.

9. Venue is appropriate in this District pursuant to 28 U.S.C. §§ 1391(a)(1).

Factual Allegations Common To All Counts

The Growth Of The Streaming Video Transport Industry

10. Telecommunications and computer networks, including the Internet, over time have expanded to allow the exchange of a broad range of information in digital form, including data, voice and, more recently, video.

11. One method of providing information over a network is via so-called "streaming media." The term "streaming media" refers to a delivery method where the end user receives content from the provider in a continuous, or "streaming" manner. As an alternative delivery mechanism, the provider could offer the content in a single file, that the user would download in complete form, and then later enjoy locally on his or her personal computer.

12. For example, streaming video content can be transported from one location to another over a network using Internet Protocol (IP) "packets." The term "packet" refers to a network communications method that splits data traffic -- digital representations of text, sound, or video data -- into discrete pieces, called "packets." These packets are then routed over the network, and the various packets that make up a single message may take different routes over the network before they are re-assembled and presented to a user at their destination.

13. Technologies that use these IP packets to transport streaming video include "Video over IP," "Video On Demand," and Internet TV or "IPTV."

14. Although splitting network traffic into packets – or "packetizing" the traffic -- results in a number of efficiencies and other benefits, the packetized nature of the information can present drawbacks.

15. For example, with respect to a digital video stream, the loss or delay of a video packet may result in a "frozen frame," a blank screen, or in tiling, pixelization, or other defects in the presentation of the stream. Streaming video,

therefore, presents real-time data transport requirements that are highly sensitive to data loss and delivery-time distortion.

16. Moreover, a network may be simultaneously hosting numerous video streams and, particularly where a large network is involved, the potential number of the failure points can be extensive.

17. In sum, data loss and delivery time distortion (among other causes) seriously affect the quality and thus the value of a video stream.

18. Industry participants – including network operators, network equipment manufacturers, and others -- now understand the importance of these parameters, the importance of testing and monitoring equipment and services with respect to these parameters, and the importance of relying on standards with respect to these parameters, to allow comparisons between approaches.

19. Moreover, with proper structures in place and data available, downstream equipment can compensate for certain upstream defects in the packetized video stream, properly buffer the stream, and thus "remedy" the stream on presentation to the end user.

20. With these developments and improvements, the streaming video services industry has experienced considerable growth, and expects considerable further growth.

21. For example, some commentators project that IPTV subscribers will increase from 12.1 million subscribers in 2007 to 60.2 million subscribers in 2012. Others note that already approximately fifty percent (50%) of all network traffic is comprised of streaming video.

The Streaming Video Transport Industry In The Early 2000s

22. In the early 2000s, industry participants were only beginning to explore the transport of digital video streams.

23. It was unclear at the time what criteria manufacturers, operators, and users would use to evaluate the quality of streaming video networks and services, and what if any standards would be applied.

24. In the early 2000s, therefore, the industry was largely undeveloped.

IneoQuest's Business; IneoQuest Innovates Key Early Solutions for Streaming Video Transport

25. Beginning in the early 2000s, the plaintiff IneoQuest was responsible for (a) determining the key parameters for evaluating streaming video; (b) developing the now industry-standard "Media Delivery Index" or "MDI" used to score the quality of a video stream; and (c) pioneering a range of technical solutions for start-to-finish video quality, service and revenue assurance.

26. IneoQuest has become a leading global supplier of end-to-end video quality, service and revenue assurance solutions for cable, satellite and telco service providers.

27. IneoQuest provides unified business solutions that audit, monitor, analyze and troubleshoot digital video. The company's products cover pre-deployment preparation in the lab and field-trial phases, as well as complete end-to-end monitoring and service assurance in the post deployment phases of a streaming video network implementation.

28. Before the industry began to focus on these issues, IneoQuest began its work on digital video solutions. For example, by 2003 IneoQuest had added features to its products to support Video over IP.

29. This feature-set included the unique ability to generate and playback an MPEG video file over IP. This real video feature set was particularly desirable for customers because it allowed the customers (such as customers of Cisco Systems, Inc.) to see -- literally on a TV -- the video stream either working smoothly or with its defects.

30. By 2004, IneoQuest had also formulated its Media Delivery Index ("MDI") and, with Cisco Systems, Inc. ("Cisco") had placed the MDI in the form of a Request for Comments ("RFC") to the Internet Engineering Task Force ("IETF"), an international group of industry participants concerned with the architecture and operation of the Internet. The MDI is a measurement that can be used as a diagnostic tool or a quality indicator for monitoring a network designed to deliver applications such as streaming video (and other information) that is sensitive to arrival time and packet loss. IneoQuest, with Cisco, described this measure in RFC 4445.

31. IneoQuest had developed unique technology for isolating faults across a live network. To accomplish this result, IneoQuest distributed probes through the network, and measured expected IP flows to determine the source of the faults. This concept and its implementation were unique in the industry.

32. Finally, by 2004, IneoQuest had developed both (i) pre-deployment solutions, which involve testing equipment and technology before these assets are put into production, and (ii) post-deployment solutions, which involve monitoring an installed network and its performance, in production. This feature set was unique in the industry.

The Importance of IneoQuest's Intellectual Property Assets

33. A significant portion of IneoQuest's value was, and is represented by its intellectual property assets, and by its "first innovator" status in the field.

34. From the outset, IneoQuest has taken proper care to protect these intellectual property assets. For example, to protect its confidential information and its trade secrets (collectively, "trade secrets"), IneoQuest has in place physical access controls in its offices. These controls include physically restricting access to company assets, requiring visitors to sign-in and retaining a log of visitors, and permitting visitors to access offices and lab space only with a company escorts. The company also employs technical access controls for its sensitive digital assets

and its networks. These include password controls, firewalls, limited privileges to certain information, and similar technical protections.

35. In addition, IneoQuest instructs its employees on the proper handling of trade secrets and other intellectual property assets, and requires that employees sign appropriate, protective agreements if they are to be exposed to the development or use of sensitive intellectual property assets.

36. In addition, in agreements with licensees of its intellectual property assets and with purchasers of its hardware solutions, IneoQuest prohibits users from reverse-engineering IneoQuest proprietary technology from the device at issue, consistent with applicable legal requirements.

37. IneoQuest also requires appropriate non-disclosure and confidentiality protections in agreements where a third party may have access to IneoQuest trade secrets. For example, IneoQuest requires potential development partners, and other parties interested in its technology, to sign protective non-disclosure agreements, before IneoQuest discloses such materials.

38. IneoQuest, therefore, takes proper precautions to safeguard its trade secrets.

39. Finally, for those novel intellectual property assets where trade secret protection may not be optimal, and in other appropriate circumstances, IneoQuest pursues patent protection.

Ixia's Business; Ixia Is Established In Data And Voice Transport, And Seeks To Enter The Field Of Video Transport

40. By 2004, Ixia had established a presence in the field of pre-deployment testing for data and voice network equipment.

41. By 2004, however, Ixia had largely been unsuccessful in entering the field of streaming video transport. Ixia was not in the video monitoring market (covering post-deployment activities), and Ixia was well behind in the video testing market (covering pre-deployment activities). Although Ixia had worked on a video

testing product, Ixia had not yet fielded the product, and its performance was uncertain.

42. Yet Ixia sought the so-called "Triple-Play," the term used in the industry to refer to the sought-after goal of providing transport solutions for (i) data, (ii) voice, and (iii) video applications, in a range of networks and with varying levels of congestion.

43. By 2004, industry participants had begun to distinguish between two general types of video streams: (i) a viewable video stream, which represented the actual video stream on the network equipment at issue, and which a tester or other user could view on a monitor (such as a TV), and (ii) a synthetic video stream, which emulated features of an actual video stream but was not the actual stream.

44. As of 2004, Ixia did not have the capability to generate viewable video, and had the ability only to generate lower quality, synthetic emulations of viewable video. On information and belief, Ixia's customers were demanding that Ixia's equipment provide an ability to test more realistic viewable video.

45. Ixia believed that using simulated video packets provided the same benefits to its customers as real video packets, and Ixia sought to convince its customers of this view.

46. On information and belief, at the time Ixia's customer base included (a) manufacturers of network routers and switches, and (b) cable companies and broadcast companies. On information and belief, the router and switch manufacturers did not object as strongly to Ixia's lack of real video, because testing emulated signals in the lab can be adequate. The cable companies and broadcast companies, however, demanded "live" viewable video for their testing.

47. As Ixia worked to overcome the challenges presented by its customer's demands, Ixia learned from its customers that IneoQuest was offering strong solutions in streaming video.

Ixia Realizes The Value of IneoQuest's Technology, And The Threat IneoQuest Poses

48. One of Ixia's core customers is Cisco, which designs and sells networking and communications services and technology, including routers for packet-switched networks. For the fiscal year ending July 2008, Cisco reported revenues of over $35 billion.

49. On information and belief, from 2004 to the present, Cisco has represented approximately twenty to thirty-five percent (20-35%) of Ixia's total revenues, and Cisco was, and is, Ixia's largest, and most important client.

50. In mid 2004, Ixia learned that Cisco was interested in purchasing IneoQuest's products for streaming video. As Ixia further investigated this fact, upon information and belief, Ixia became increasingly concerned: first, due to the strength of IneoQuest's technology; second, due to Cisco's interest in IneoQuest's technology; and, finally, due to Ixia's lack of a viable product and feature-set to compete with IneoQuest.

51. Ixia addressed its concerns by conducting a detailed investigation of IneoQuest.

52. For example, Ixia analyzed the pricing and public-facing feature-set of IneoQuest's products. Ixia determined that Ixia's video solution did not contain the feature-set and technology that customers were beginning to demand, and that were contained in IneoQuest's products. Moreover, Ixia determined that it was offering its video "solutions" at prices many multiples of IneoQuest's prices. Ixia determined, therefore, that IneoQuest was offering better products, at lower prices.

53. Ixia also investigated the MDI measure that IneoQuest was working to establish as an industry standard. For example, Ixia obtained from IneoQuest a copy of RFC 4445, which described the MDI measure for streaming video (and other streaming media).

54. On information and belief, Ixia noted that IneoQuest had presented RFC 4445 to the IETF jointly with Cisco. Also on information and belief, Ixia engaged its engineering department and product managers to analyze RFC 4445, and MDI. Ixia also begin to analyze the level of acceptance of MDI as a standard in the industry.

55. Ixia learned that, like Cisco, Comcast Corporation ("Comcast") was working with IneoQuest on MDI technology. Like Cisco, Comcast was, and is, a key participant in the streaming video industry. Comcast's business focuses on the delivery of video, voice, and high-speed internet services over an advanced, fiber-optic-based network. By 2007 Comcast had become, in the United States, the largest cable and residential high-speed Internet provider, and the fourth-largest phone company. In 2007, Comcast reported that it provided these services to more than 42 million households, and generated total revenues of over $30 billion.

56. In sum, upon information and belief, Ixia determined that its video technology was not answering its customers' requirements, that this technology (even holding aside its technical deficiencies) was not competitively priced, and that its key customers, particularly Cisco, were going to buy IneoQuest's solution unless Ixia had a response.

57. The possibility of these purchases particularly concerned Ixia because, if these key customers adopted IneoQuest's solution early in the market's evolution, it would be likely that these customers would remain with IneoQuest, to the exclusion of Ixia.

58. In assessing its response to the challenge posed by IneoQuest's better and cheaper streaming video solutions, Ixia early on determined that it would not negotiate a relationship with IneoQuest whereby Ixia would "bundle" IneoQuest hardware with Ixia hardware. Ixia thus internally rejected a structure whereby Ixia would act as a "value added reseller" or other reseller.

59. Despite its internal decision to reject a reseller or other "bundling" type relationship, Ixia determined that it must find a way to adopt IneoQuest's technology in its product offering.

60. Over time, Ixia then formulated and implemented a plan to acquire the trade secrets underlying IneoQuest's technology, and adopt this technology in Ixia's products, without IneoQuest's permission and in violation of Ixia's non-disclosure and non-use obligations.

The Parties Enter the 2004 Non-Disclosure Agreement, And Exchange Trade Secret Information

61. In late June, 2004, Ixia contacted IneoQuest and proposed that the parties meet to discuss potential ways in which Ixia and IneoQuest might work together.

62. Although Ixia had gathered substantial publicly-available information concerning IneoQuest from IneoQuest's website, Ixia had a number of inquiries that required access to IneoQuest's non-public, trade secret information.

63. Consistent with its practice, IneoQuest would not disclose the additional information without a non-disclosure agreement in place.

64. Moreover, Ixia indicated that it planned to disclose to IneoQuest information that Ixia deemed confidential and that concerned Ixia's industry position, and plans concerning video streaming.

65. Accordingly, the parties signed a mutual non-disclosure agreement, with an effective date of July 7, 2004 (the "2004 Non-Disclosure Agreement"). A true and accurate copy of the 2004 Non-Disclosure Agreement is attached as Exhibit 1.

66. The 2004 Non-Disclosure Agreement prohibits a party from using confidential information of the other for any purpose other than the purpose of engaging in discussions concerning a potent transaction.

67. The parties then scheduled a face-to-face meeting for July 23, 2004 (the "July 2004 Meeting"). The meeting was designed to discuss a potential relationship, and exchange trade secret information to inform their decisions concerning this potential relationship.

68. Consistent with the provisions of the 2004 Non-Disclosure Agreement, the parties identified in writing the confidential information they intended to discuss at the meeting, via an agenda dated July 21, 2004.

69. The July 23, 2004 meeting had a business component, and a technical component.

70. The business component consisted of a confidential discussion of IneoQuest's plans for the company, the company's product sales per month, the equity ownership the company, whether its owners were interested in selling the company, and related points. The parties also confidentially discussed their interests in working together, and possible structures for the relationship. For example, Ixia learned that IneoQuest had gained primary traction through network monitoring rather than equipment testing. IneoQuest's focus on monitoring made IneoQuest a more attractive business partner, because it primarily supplemented rather than competed in Ixia's markets, which focused on testing. Ixia realized, however, that IneoQuest's business was a mix of network monitoring and pre-deployment testing or lab testing. Finally, Ixia provided confidential disclosures concerning its then-current position in the video market, and its plans.

71. The technical component consisted of confidential disclosures by IneoQuest concerning how IneoQuest had architected its product, and specifics concerning IneoQuest's software and hardware solutions. For example, IneoQuest made confidential disclosures concerning the capture/replay generation capability of its product, which was the key technique for creating a realistic video flow. IneoQuest also confidentially disclosed the power requirements of its products. IneoQuest also confidentially disclosed details concerning its approach of placing

probes at various points in a network and monitoring video quality from an operations center.

72. IneoQuest believed it was in the parties' mutual interests for Ixia to resell IneoQuest's products, or to include an IneoQuest-manufactured card in its devices. With Ixia's urging, IneoQuest was therefore willing to disclose, and did disclose a wealth of confidential information to allow Ixia to assess in detail whether a relationship would make sense from a technical standpoint.

73. At Ixia's urging, IneoQuest also provided a wealth of confidential information to educate Ixia concerning the streaming video market, and its potential. The subsequent success of this market – in the manner IneoQuest disclosed -- underscores the value of the confidential business information IneoQuest provided to Ixia at this meeting.

74. This meeting caused Ixia to re-assess its approach to the market for streaming video transport. For example, before this meeting, Ixia felt video flows were not important to analyze on a per flow basis. Ixia also believed that synthetic video should be sufficient for its customers. Ixia, in addition, was not focused on adopting MDI measures. Based on IneoQuest's confidential disclosures, however, Ixia fundamentally changed its position.

75. Moreover, based on IneoQuest's extensive, confidential technical disclosures, Ixia concluded that IneoQuest had designed the device that the broader market of network-level customers sought. More important, Ixia concluded that IneoQuest had developed the technology and feature-set that Ixia would need to in order to enter the video transport testing segment.

76. Within roughly three weeks after the July 2004 Meeting, Ixia had transcribed the material confidential information IneoQuest had disclosed during the July 2004 meeting, in the form of a "requirements document" for designing streaming video products (the "2004 Design Document"). Ixia called this

undertaking – based on IneoQuest's trade secret technology – Ixia's "Project Hollywood."

77. Ixia's 2004 Design Document discusses video over IP testing, and directly references IneoQuest. In this Design Document, Ixia recognized that IneoQuest's video solution was currently uncontested in the market. Ixia concluded (a) that it needed a fast time-to-market for its competing solution, and (b) that it needed a blocking maneuver to prevent IneoQuest from entrenching its uncontested position in the market.

78. Ixia could not have produced the 2004 Design Document, and could not have produced the Design Document when it did without the highly valuable, core trade secret disclosures from IneoQuest.

Ixia Continues Discussions To Obtain Additional Confidential Information From IneoQuest, And Furthers Its Efforts To "Block" IneoQuest

79. After creating the 2004 Design Document, based on IneoQuest's trade secret disclosures, Ixia determined to adopt the technical and business approach IneoQuest had disclosed.

80. Ixia had not, however, determined the "path" it would take to adopt this approach.

81. Through the late fall and early winter of 2004, upon information and belief, Ixia either (a) was ambiguous about whether to work with IneoQuest, and compensate IneoQuest for its technology and business insights, or (b) had already determined to exclude IneoQuest and "go it alone" (while relying on the 2004 Design Document and other materials created with IneoQuest core trade secrets).

82. In either event, by October 2004 Ixia had more than sufficient information from IneoQuest, under the parties' 2004 Non-Disclosure Agreement, to allow Ixia to decide whether to proceed with the proposed transaction. Ixia, however, continued to push IneoQuest for more confidential information.

83. In meetings in October and November, 2004, despite Ixia's at best "ambiguous" position concerning a working relationship with IneoQuest, Ixia management continued to extract further trade secret from IneoQuest. This information comprised additional disclosures concerning IneoQuest's specific technology and product implementation, as well as disclosures concerning IneoQuest's market insights. For example, Ixia obtained from IneoQuest during this period confidential information concerning IneoQuest's gross profit margin, cost of component parts, and number of employees.

84. In addition to extracting further confidential information from IneoQuest – at a time when Ixia was at best "on the fence" about including IneoQuest in its 2004 Design Document plans -- Ixia succeeded in tying up IneoQuest's business focus.

85. Ixia stated that it would provide a "term sheet" to IneoQuest, if IneoQuest would sign a "no-shop" agreement. Under this agreement, called an "Exclusive Negotiation Agreement," IneoQuest and Ixia agreed that they would not negotiate with others concerning an intellectual property license, sale, lease, or other disposition of a significant portion of the assets of IneoQuest (the "No-Shop Agreement").

86. IneoQuest signed the No-Shop Agreement on October 26, 2004. IneoQuest proposed to Ixia terms for a relationship, under the No-Shop Agreement and the parties' 2004 Non-Disclosure Agreement. On information and belief, Ixia conceded that these terms were reasonable.

87. Ixia, meanwhile, continued with its secret plans to develop (or acquire) a streaming video solution that was the equivalent of IneoQuest's solution, to the exclusion of IneoQuest.

88. By late December or early January, Ixia had formally decided to reject any business relationship with IneoQuest. Ixia decided, instead, to "develop" a

streaming video solution based on the 2004 Design Document, which in turn was based on IneoQuest's trade secrets.

89. Ixia did not inform IneoQuest of Ixia's decision to reject any business relationship with IneoQuest.

Ixia Misappropriates IneoQuest's Trade Secrets, And Interferes With IneoQuest's Key Customers

90. Roughly simultaneous with this decision, Ixia completed a "roadmap" for its business and development approach to streaming video. Under this roadmap, Ixia stated internally that it would implement video streams in its IxLoad and IxChariot products and, among other goals, Ixia planned to add Video over IP support to the IxLoad product.

91. More importantly, Ixia determined to include in its offerings MDI-- IneoQuest's technology – by the second half of 2005.

92. On information and belief, Ixia spent time deliberating whether to include IneoQuest's MDI technology in its products, and to rely on the trade secret disclosures from IneoQuest that underlay Ixia's 2004 Design Document. Ixia determined that simply "going along with MDI," and adopting the trade secret information it had already obtained from IneoQuest, would allow it to implement the new functionality and feature-set into its products quickly.

93. Ixia was under considerable pressure to include IneoQuest's MDI technology in its products. On information and belief, Ixia believed by April 2005 that MDI capabilities needed to be added to IxChariot immediately, due to customer demand.

94. Indeed, on information and belief, a number of Ixia's customers stated that they would continue to do business with Ixia in the video area, but only if Ixia were able to offer all of the features IneoQuest offered.

95. To collect further information concerning IneoQuest's products –even beyond the sensitive trade secrets it had already obtained – on information and

belief Ixia purchased IneoQuest equipment and, in violation of the end user agreement for this equipment, reverse-engineered the devices.

96. Ixia thus worked quickly to meet these customer requirements, using trade secrets misappropriated from IneoQuest.

97. Although Ixia was working to incorporate in Ixia products (without compensation and wrongfully) IneoQuest's technology, including its MDI measure, Ixia did not savor the prospect of supporting MDI. Ixia believed that this might "legitimate" and "validate" IneoQuest, a company that, on information and belief, Ixia now sought to put out of business. Accordingly, Ixia sought to describe its adoption of MDI in a manner that would discredit IneoQuest.

98. On information and belief, by July 2005, or roughly only seven months since commencing "development," Ixia had implemented IneoQuest's trade secret technology in IxChariot, which was able to generate MDI figures.

99. While Ixia's engineers worked to implement IneoQuest's trade secrets into Ixia's products, Ixia management worked to forestall customer purchases, to avoid these customers choosing IneoQuest over Ixia.

100. Ixia falsely informed customers as to the state of its progress in meeting their needs for IneoQuest's technology. Ixia's sale force complained over the difficulty of "selling" an Ixia product that did not exist.

101. Ixia allowed and encouraged references to the effect that IneoQuest's feature-set had been "branded" under Ixia's trademarks, and included within Ixia's products.

102. Ixia convinced its customers, in breach of their non-disclosure obligations to IneoQuest, to inform Ixia of IneoQuest's movements and approaches in the market. With this information, Ixia sought to anticipate, and block IneoQuest's marketing efforts and technical demonstrations.

103. With these efforts, Ixia succeeded in convincing purchasers to postpone their purchasing decisions, to allow Ixia to put forward products "competitive" with IneoQuest.

104. Ixia thus (a) created a video generation feature set; (b) modified IxLoad to analyze multiple video strings, analyze them, and apply MDI measures; and (c) incorporated distributed probes, across a live network for the purpose of fault isolation by measuring an expected IP flow, all based on trade secret information obtained from IneoQuest.

IneoQuest Discovers Ixia's Wrongdoing

105. IneoQuest discovered Ixia's wrongdoing in mid-August 2008.

106. As this point, IneoQuest management obtained access to documents and other materials that described Ixia's activities, plans, and other previously undisclosed actions.

107. This information, which had wrongfully been withheld from IneoQuest, demonstrated the wrongdoing described above.

108. After further diligence, IneoQuest promptly acted upon this new information, and informed Ixia of the present claims.

IneoQuest's Patent

109. On January 22, 2008, United States Patent Number 7,321,565 (the "'565 Patent"), entitled "System and Method for Analyzing the Performance of Multiple Transportation Steams of Streaming Media in Packet-Based Networks," was duly issued to IneoQuest, as assignee of the named inventors. A true and accurate copy of the '565 Patent is attached as Exhibit 2.

110. Prior to issuance, but after the filing of its patent application, IneoQuest disclosed the invention described and claimed in the '565 Patent (the "Invention") to Ixia under Non-Disclosure Agreements, and RFC 4445.

111. IneoQuest disclosed the Invention to Ixia so that Ixia could consider incorporating the Invention into its products and systems under a commercial relationship.

112. Thereafter, Ixia notified IneoQuest that it was not interested in the Invention. Despite this representation, Ixia uses the Invention at least in its IxLoad, IxRave, and IxChariot products.

113. Upon information and belief, Ixia became aware that the '565 Patent had issued at or around the time of issuance, was aware that it was using the Invention as disclosed by IneoQuest and as claimed in the '565 Patent, and continued to infringe the '565 Patent thereafter.

114. IneoQuest is not obligated, under RFC 4445 or standards-related structures, to provide licenses to industry participants with respect to the practice of the Invention.

115. Moreover, although IneoQuest has granted licenses to certain industry participants with respect to RFC 4445, and although these licenses include (among other provisions) favorable, royalty-free grants to these licensees (the "Favored Licensees"), IneoQuest bears no obligation at law or in equity to treat Ixia in any sense as a Favored Licensee.

116. Accordingly, Ixia infringes the invention described and claimed in the '565 Patent.

Ixia's Wrongs Have Caused Significant Damage To IneoQuest

117. Ixia's wrongdoing has caused substantial damage to IneoQuest.

118. First, IneoQuest has suffered damages in terms of lost direct sales. Industry participants that would have purchased IneoQuest's video generation solution instead purchased a misappropriated and infringing "Ixia solution."

119. Second, the sale of the video streaming products at issue generates significant "follow-on" sales of related products and services. Ixia's wrongdoing deprived IneoQuest of these sales.

120. Third, Ixia's blocking of IneoQuest in the market allowed others, in addition to Ixia, to reduce the advantage IneoQuest held through its "first-innovator" status.

121. Fourth, by disrupting its customer relationships and its prospective customer relationships, by misappropriating its trade secrets, by unfairly competing with it, and by infringing on its patent rights, Ixia has gravely harmed IneoQuest.

122. Ixia's conduct, for the above reasons and others, has resulted in significant damage to IneoQuest

Count I

Infringement of U.S. Patent No. 7,321,565

123. IneoQuest repeats and incorporates by reference the allegations set forth in paragraphs 1 through 122.

124. The '565 Patent is valid and enforceable.

125. IneoQuest owns all requisite right, title and interest in and to the '565 Patent.

126. Ixia has infringed and continues to infringe '565 Patent, either directly, by contributory infringement, or by inducing others to infringe, through its marketing and other efforts.

127. Ixia has willfully infringed the '565 Patent, acting in an objectively reckless manner upon publication of the '565 Patent, and then upon issuance of the ‘565 Patent.

128. As a direct result of Ixia’s infringement, IneoQuest has suffered, and will continue to suffer damages, irreparable harm and impairment of the value of its patent rights.

129. IneoQuest is entitled to recover from Ixia the damages sustained by IneoQuest as a result of Ixia’s wrongful acts in an amount subject to proof at trial.

Count II

Breach of Contract

130. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 129 as if fully set forth herein.

131. The parties entered into the 2004 Non-Disclosure Agreement.

132. The 2004 Non-Disclosure Agreement is valid and enforceable, and obligates Ixia to respect the confidentiality of, and not to use IneoQuest's confidential and trade secret information.

133. IneoQuest performed its obligations under each applicable provision of the 2004 Non-Disclosure Agreement.

134. Defendant Ixia breached the 2004 Non-Disclosure Agreement by (a) taking information that constituted IneoQuest confidential information under the Agreement, (b) using this information to develop streaming video products and services competitive with IneoQuest's products and services; and (c) using this information to improperly attack and compete with IneoQuest in the streaming video market.

135. As a direct and proximate result of Ixia's breach of the 2004 Non-Disclosure Agreement, IneoQuest has suffered significant and irreparable damage.

Count III

Trade Secret Misappropriation In Violation Of The Uniform Trade Secret Act: CA Civil Code §3426

136. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 135 as if fully set forth herein.

137. After signing the 2004 Non-Disclosure Agreement in order to evaluate the possibility of a transaction between the parties, Ixia became intimately familiar on a confidential basis with all material aspects of IneoQuest's operations, and was given access to and gained knowledge of IneoQuest's trade secrets, both with respect to IneoQuest's technical and trade secret solutions in the streaming

video market, and with respect to IneoQuest's business plans and evaluations with respect to this market.

138. This trade secret information had economic value in that IneoQuest invested a substantial amount of time, energy, and money to develop the information and maintain its secrecy.

139. IneoQuest took reasonable steps to protect the secrecy of the trade secret information.

140. Ixia misappropriated the above described trade secrets.

141. Defendant Ixia's wrongful use and disclosure of IneoQuest's trade secrets has given Ixia a substantial and unearned competitive advantage, to which it is not entitled.

142. IneoQuest has suffered significant damage as a result of defendant Ixia's misappropriation. Such damages will continue until defendant Ixia is enjoined from using IneoQuest's trade secret information.

143. Ixia's misappropriation was willful and malicious, and Ixia intended by its wrongful conduct to cause serious damage to IneoQuest's streaming video business. Defendant Ixia's conduct justifies an award to IneoQuest of exemplary damages under Civil Code § 3426.3 and of attorneys' fees under Civil Code § 3426.4.

Count IV

Intentional Interference with Contract

144. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 143 as if fully set forth herein.

145. IneoQuest had enforceable non-disclosure agreements with third party customers that obligated these entities to preserve confidential information IneoQuest disclosed concerning its products, and its activities in the streaming video market.

146. Defendant Ixia knew that IneoQuest had such agreements with customers.

147. In order to wrongfully block IneoQuest from the market, and improperly obtain business from IneoQuest's customers, defendant Ixia engaged in conduct intended to disrupt the contractual relationships between IneoQuest and its customers by convincing such customers to share IneoQuest confidential information with Ixia, and by making false statements concerning its technology and the technology of IneoQuest.

148. IneoQuest customers, in breach of non-disclosure obligations, shared IneoQuest confidential information with Ixia, at Ixia's urging.

149. In addition, based on Ixia's false statements concerning its technology and IneoQuest's technology, IneoQuest's customers did not conduct the level of business with IneoQuest which they would have conducted, had Ixia acted properly.

150. As a proximate result of this wrongful conduct by defendant Ixia, Ixia obtained further valuable IneoQuest confidential information, and disrupted IneoQuest's relationship with important clients.

151. IneoQuest has been substantially damaged by Ixia's wrongdoing in this regard, in an amount to be proven at trial.

Count V

Common Law Unfair Competition

152. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 151 as if fully set forth herein.

153. Defendant Ixia's acts of misappropriating IneoQuest's trade secrets for use in a competing business constitutes unfair competition.

154. Defendant Ixia's efforts to "block" IneoQuest from the market, false statements to customers concerning Ixia's products and IneoQuest's products, and

implemented plans to put IneoQuest "out of business" constitute unfair competition.

155. These acts by defendant Ixia violate fundamental public policy of the State of California, and constitute unfair competition.

156. As a proximate result of defendant Ixia's conduct, IneoQuest has suffered, and will continue to sustain substantial injury and damages in an amount to be determined at trial.

Count VI

Unfair Competition in Violation of CA Business and Professions Code §§17200, et seq

157. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 156 as if fully set forth herein.

158. In the course of competing with IneoQuest, defendant Ixia used (a) the confidential information it obtained from IneoQuest under the 2004 Non-Disclosure Agreement, in violation of its terms, and (b) the confidential information it wrongfully obtained from IneoQuest's customers.

159. These unlawful uses by defendant Ixia of IneoQuest's confidential information have given Ixia a substantial and unearned competitive advantage, to which it is not entitled.

160. Defendant Ixia's efforts to "block" IneoQuest from the market, false statements to customers concerning Ixia's products and IneoQuest's products, and implemented plans to put IneoQuest "out of business" constitute unfair competition.

161. These actions by Defendant Ixia are unlawful based on Civil Code § 3426.1, et seq. and otherwise, and constitute unfair competition in violation of Business and Professions Code Section 17200, et seq.

162. These actions by Defendant Ixia are fraudulent and deceitful, and constitute unfair competition in violation of Business and Professions Code Section 17200, et seq.

163. As a proximate result of defendant Ixia's conduct, IneoQuest has suffered and will continue to sustain substantial injury and damages, in an amount to be determined at trial.

164. Defendant Ixia's actions were willful and malicious. IneoQuest, accordingly, is entitled to an award of reasonable attorneys' fees pursuant to Civil Code § 3426.4.

Count VII

Intentional Interference with Prospective Economic Advantage

165. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 164 as if fully set forth herein.

166. IneoQuest is a leader in the field of streaming video, and had existing and ongoing relationships with third parties to provide products and services in this field.

167. IneoQuest had a reasonable expectation that those relationships were likely to result in future business and/or continuing economic advantage to IneoQuest.

168. Defendant Ixia knew that IneoQuest had such relationships with third party customers for the provision of streaming video products and services.

169. Defendant Ixia intentionally engaged in conduct designed to give defendant Ixia an unfair competitive advantage against IneoQuest and intended to disrupt IneoQuest's relationships with third party customers and potential customers. That conduct includes, but is not limited to: (a) Ixia's use of IneoQuest confidential information (obtained from IneoQuest and its customers) to improperly compete with IneoQuest and influence prospective customers; (b) Ixia's false claims that its products contained a feature-set comparable to IneoQuest's;

and (c) its improper efforts to undermine industry acceptance of the MDI measure through, among other wrongful conduct, its false claims concerning IneoQuest's products and concerning Ixia's own products and purported product features.

170. As a proximate result of defendant Ixia's conduct, IneoQuest has been deprived of relationships with these third party customers and prospects.

171. IneoQuest has been damaged in a sum to be proven at trial.

Count VIII

Negligent Interference with Prospective Economic Advantage

172. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 171 as if fully set forth herein.

173. IneoQuest is a leader in the field of streaming video, and had existing and ongoing relationships with third parties to provide products and services in this field.

174. IneoQuest had a reasonable expectation that those relationships with third party customers and potential customers were likely to result in future business and/or continuing economic advantage to IneoQuest.

175. Defendant Ixia knew that IneoQuest had such relationships with third party customers.

176. In the exercise of reasonable care, Ixia should have known that its conduct would damage IneoQuest's relationships with such third party customers. Such conduct includes, but is not limited to: (a) Ixia's use of IneoQuest confidential information (obtained from IneoQuest and its customers) to compete with IneoQuest and influence prospective customers; (b) Ixia's false claims that its products contained a feature-set comparable to IneoQuest's; and (c) Ixia's efforts to undermine industry acceptance of the MDI measure.

177. Defendant Ixia knew, or should have known, that if it negligently interfered with these relationships, IneoQuest would foreseeably lose some or all of its probable future economic benefit from such relationships.

178. As a proximate result of defendant Ixia's conduct, IneoQuest has been deprived of relationships with these third party customers and prospects.

179. IneoQuest has been damaged in a sum to be proven at trial.

Count IX

Breach of Confidence

180. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 179 as if fully set forth herein.

181. Under the 2004 Non-Disclosure Agreement, IneoQuest conveyed secret information to defendant Ixia.

182. Under the terms of the 2004 Non-Disclosure Agreement, defendant Ixia knew the information it would receive from IneoQuest was secret and confidential. Defendant Ixia agreed to the terms of the 2004 Non-Disclosure Agreement and voluntarily accepted the confidential and secret information under the condition that it would keep such information confidential pursuant to Sections 3, 4, 6 and 7 of the 2004 Non-Disclosure Agreement.

183. Defendant Ixia breached the 2004 Non-Disclosure Agreement and used the confidential information to develop products and services to directly compete with IneoQuest, and to interfere in IneoQuest's actual and prospective customer relationships.

184. As a proximate result of defendant Ixia's conduct, IneoQuest has been damaged in a sum to be proven at trial.

Count X

Misappropriation of Work Product

185. IneoQuest restates and re-alleges the allegations contained in Paragraphs 1 through 185 as if fully set forth herein.

186. IneoQuest invested significant time, money, and expertise in developing its trade secrets and other confidential information.

187. Defendant Ixia used IneoQuest's trade secrets and confidential information in violation of the 2004 Non-Disclosure Agreement between the parties and without compensating IneoQuest.

188. IneoQuest has suffered damages as a result of Ixia's actions.

Requested Relief

WHEREFORE, IneoQuest prays that this Court enter judgment:

(a) That Ixia has infringed the '565 Patent;

(b) That Ixia, and its officers, agents, servants, employees, subsidiaries, attorneys, and those acting in concert with it, be enjoined from committing the aforesaid acts of infringement;

(c) That Ixia be ordered under Count I to pay damages adequate to compensate IneoQuest for Ixia's infringement of the '565 Patent, along with prejudgment interest;

(d) That Ixia be ordered to pay enhanced damages and attorneys' fees pursuant to 35 U.S.C. §§ 284 and 285 under Count I;

(e) That Ixia be ordered to pay damages in an amount to be set at trial on Counts II through X;

(f) That Ixia be enjoined from continuing to use and benefit from IneoQuest's trade secrets and confidential information, under Counts II through X;

(g) That Ixia be ordered to pay IneoQuest's attorney's fees in this action, as required under the 2004 Non-Disclosure Agreement and as provided by law; and

(h) That IneoQuest be awarded its costs, and such other and further relief as the Court deems just and proper.

Dated: November 25, 2008

HOLLAND & KNIGHT LLP

By: ______________________________
Richard T. Williams

Attorneys for Plaintiff IneoQuest
Technologies, Inc.

Of Counsel
Ieuan G. Mahony (BBO #552349)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

DEMAND FOR JURY TRIAL

Plaintiff Attorneys for Plaintiff IneoQuest Technologies, Inc. hereby demands a jury trial as to all issues so triable.

Dated: November 25, 2008

HOLLAND & KNIGHT LLP

By: ______________________________
Richard T. Williams

Attorneys for Plaintiff IneoQuest
Technologies, Inc.

Of Counsel

Ieuan G. Mahony (BBO #552349)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

EXHIBIT 1

MUTUAL NONDISCLOSURE AGREEMENT

This Agreement is made as of this 7 xxth day of July ~~xx~~, 2004, by and between Ixia, a California corporation, located at 26601 West Agoura Road, Calabasas, California 91302 ("Ixia"), and IneoQuest Technologies, Inc, a Delaware Corporation, located at 170 Forbes Blvd, Mansfield, Massachusetts 02048 ("IneoQuest").

RECITALS:

WHEREAS, Ixia and IneoQuest wish to exchange certain information of a confidential or proprietary nature concerning the business, operations and/or assets of their respective companies in connection with their consideration of and/or negotiations regarding a possible transaction between the parties hereto;

WHEREAS, for the purposes set forth herein, either Ixia or IneoQuest ("Discloser") may disclose, from time to time, such confidential or proprietary information to the other party hereto ("Disclosee") on a confidential basis; and

WHEREAS, as a condition to such disclosure, Disclosee agrees to treat such information concerning Discloser in accordance with the terms and provisions of this Agreement and to take or abstain from taking certain actions set forth in this Agreement;

NOW, THEREFORE, in consideration of the foregoing premises and the following promises and covenants and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

AGREEMENT:

1. Accuracy of Recitals. Each of the parties hereto acknowledges that the foregoing recitals are true and correct.

2. Representatives. "Representatives," as used herein, means a party's officers, directors, employees, attorneys, accountants, consultants, financial advisors, lenders and other advisors and agents who are assisting such party in connection with a possible transaction between the parties hereto.

3. Confidential Information. "Confidential Information," as used herein, means any information or material concerning Discloser which on or after the date hereof is furnished under this Agreement by Discloser to, and is accepted by, Disclosee or its Representatives in connection with a possible transaction between the parties hereto, which is in written, graphic, recorded, photographic or any machine readable form (or oral information reduced to writing as soon as practicable after disclosure to Disclosee) and which, in any case, is conspicuously marked or labeled "Confidential," "Proprietary" or in another manner indicating its confidential and/or proprietary nature, or which in the case of oral information is specifically identified as being confidential or proprietary. The term "Confidential Information" includes all notes, analyses, compilations, studies, interpretations or other materials prepared by Disclosee or its Representatives to the extent they contain or are based

on the information furnished to Disclosee or its Representatives pursuant to this Agreement. The term "Confidential Information" does not include information which (a) is already in Disclosee's possession at the time of its disclosure by Discloser to Disclosee as shown by Disclosee's files and records; (b) is now or hereafter becomes generally known or available to the public other than as a result of a disclosure by Disclosee or its Representatives in violation of this Agreement; (c) becomes available to Disclosee on a nonconfidential basis from a source other than Discloser or any of its Representatives unless (i) Disclosee knows that such source is a party to a confidentiality agreement with Discloser or is subject to a legal or fiduciary obligation of confidentiality to Discloser, (ii) such information is subject to such agreement or obligation, and (iii) Disclosee knows that such source's disclosure of such information to Disclosee constitutes a breach of such source's confidentiality agreement with, or such source's legal or fiduciary obligation of confidentiality to, Discloser; (d) is independently developed by Disclosee without the use of any Confidential Information; (e) is furnished by Discloser to others not in a confidential relationship with Discloser without restrictions similar to or stricter than those herein on the right of the receiving party to use or disclose the Confidential Information; or (f) is received by Disclosee after written notification to, and receipt of such notification by Discloser, that Disclosee will not accept any further confidential information.

4. Nondisclosure of Confidential Information. Disclosee agrees that (a) it and its Representatives shall use the Confidential Information solely for the purpose of evaluating a possible transaction between the parties hereto; (b) Disclosee will maintain the confidentiality of the Confidential Information; and (c) Disclosee will not disclose any of the Confidential Information to any person(s) other than to Disclosee's Representatives who have a reasonable need to know such information for the purpose of evaluating a possible transaction with Discloser and who are first informed by Disclosee of the confidential nature of the Confidential Information and provided with a copy of this Agreement and agree to be bound by the terms of this Agreement as if they were parties hereto. Disclosee agrees to use reasonable efforts (including, without limitation, litigation if such litigation would be part of such reasonable efforts) to cause its Representatives to treat Confidential Information furnished by or on behalf of Discloser in accordance with this Agreement and shall be responsible for any breach of this Agreement by its Representatives.

5. Nondisclosure of Possible Transaction. Each party agrees that it and its Representatives, without the prior written consent of the other party, will not disclose to any person (other than to a person to whom such disclosure is authorized hereunder) the fact that Confidential Information has been made available to such party, the fact that discussions or negotiations are taking place concerning a possible transaction between the parties hereto or any of the terms, conditions or other facts with respect to such discussions or negotiations (including the status thereof), unless in the written opinion of counsel such disclosure is required by law and then only with as much prior notice to the other party as is practical under the circumstances. The term "person" as used in this Agreement shall be broadly interpreted to include the media and any corporation, partnership, limited liability company, group, individual or other entity.

6. Protection of Confidential Information. In the event that Disclosee or any of its Representatives are requested or required (by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoena, civil investigative demand or other similar process) to disclose any of the Confidential Information, Disclosee shall provide Discloser with prompt written notice of any such request or requirement so that Discloser may have an opportunity to seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this

Agreement. If, in the absence of a protective order or other remedy or the receipt of a waiver from Discloser, Disclosee or any of its Representatives are nonetheless in the written opinion of counsel legally compelled to disclose Confidential Information to any tribunal or else stand liable for contempt or suffer other censure or penalty, Disclosee or its Representatives may, without liability hereunder, disclose to such tribunal only that portion of the Confidential Information which counsel advises Disclosee it is legally required to disclose.

7. Return of Confidential Information. If either party decides that it does not wish to proceed with a possible transaction with the other party, then such party will promptly inform the other party of that decision. In that case, or at any time upon the request of Discloser for any reason, Disclosee will promptly deliver to Discloser all Confidential Information (and all copies thereof) furnished to Disclosee or its Representatives and then possessed by Disclosee or its Representatives. In the event of such a decision or request, all other Confidential Information prepared by Disclosee or its Representatives and then possessed by Disclosee or its Representatives shall be destroyed and no copy thereof shall be retained. Notwithstanding the return or destruction of the Confidential Information, Disclosee and its Representatives will continue to be bound by their obligations of confidentiality and other obligations hereunder.

8. Irreparable Injury; Equitable Relief. The parties hereto acknowledge and agree that any unauthorized disclosure or use by Disclosee or any of its Representatives (or any other person or entity) of any Confidential Information, or any other breach by Disclosee hereunder, will result in irreparable injury to Discloser and that Discloser shall be entitled to equitable relief, including injunction and specific performance, as a remedy for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach by Disclosee of this Agreement but shall be in addition to all other remedies available at law or equity to Discloser.

9. Accuracy of Confidential Information. Although Discloser shall endeavor to include in the Confidential Information information which Discloser believes to be relevant for the purpose of Disclosee's evaluation of a possible transaction between the parties hereto, Disclosee acknowledges and understands that, except as agreed to in writing, neither Discloser nor any of its Representatives make any representation or warranty as to the accuracy or completeness of the Confidential Information. Disclosee agrees that neither Discloser nor any of its Representatives shall have any liability to Disclosee or to any of its Representatives resulting from their use of the Confidential Information except as agreed to in writing or as imposed by law.

10. No Obligation. The parties agree that unless and until a definitive agreement regarding a transaction between the parties has been executed, neither party will be under any legal obligation of any kind whatsoever with respect to such a transaction by virtue of this Agreement except for the rights and obligations specifically agreed to herein. The parties further acknowledge and agree that each party reserves the right, in its sole discretion, to terminate discussions and negotiations with the other party at any time and for any reason or no reason.

11. Miscellaneous.

(a) No Other Parties to Benefit. This Agreement is made for the sole benefit of the parties hereto, and no other person or entity is intended to or shall have any rights or benefits hereunder, whether as a third party beneficiary or otherwise. Neither party may assign or transfer any of its rights or obligations under this Agreement without the prior written consent of the other party.

(b) Governing Law. The parties hereto acknowledge that this Agreement is executed and delivered in the State of California and agree that the laws of the State of California shall govern its interpretation and enforcement, and that any legal action arising out of or in connection with this Agreement or any breach hereof shall be brought and prosecuted in an appropriate court of competent jurisdiction within the County of Los Angeles in the State of California.

(c) Modification and Waiver. No provision of this Agreement shall be amended, waived or modified except by an instrument in writing signed by the parties hereto.

(d) Severability and Integration. Inapplicability or unenforceability of any provision of this Agreement shall not limit or impair the operation or validity of any other provision hereof. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes any prior or contemporaneous discussions, representations or agreements, whether written or oral.

(e) Litigation and Attorneys' Fees. In the event litigation arises in connection with enforcement of any provision of this Agreement, the prevailing party in such litigation shall be entitled to recover its attorneys' fees and expenses, in addition to any other relief to which it may be deemed entitled.

(f) Counterparts. This Agreement may be executed in counterparts, each of which shall be enforceable as an original, but which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the date first above-written.

IXIA	IneoQuest Technologies, Inc
By: 7/8/04	By: 7/7/04
Josh Goldstein	Print Name: Marc Todd
Principal Technologist	Print Title: Chief Executive Office & President

EXHIBIT 2

US007321565B2

(12) **United States Patent**
Todd et al.

(10) **Patent No.: US 7,321,565 B2**
(45) **Date of Patent: Jan. 22, 2008**

(54) **SYSTEM AND METHOD FOR ANALYZING THE PERFORMANCE OF MULTIPLE TRANSPORTATION STREAMS OF STREAMING MEDIA IN PACKET-BASED NETWORKS**

(75) Inventors: **Marc Todd**, Foxboro, MA (US); **Jesse D. Beeson**, Franklin, MA (US); **James Welch**, Mashpee, MA (US)

(73) Assignee: **Ineoquest Technologies**, Mansfield, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 873 days.

(21) Appl. No.: **10/604,997**

(22) Filed: **Aug. 29, 2003**

(65) **Prior Publication Data**

US 2005/0047333 A1 Mar. 3, 2005

(51) **Int. Cl.**
H04L 1/00 (2006.01)
H04J 1/16 (2006.01)

(52) **U.S. Cl.** **370/253**; 370/235

(58) **Field of Classification Search** 370/252–253, 370/401, 229–240; 709/224
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,738,813	B1 *	5/2004	Reichman	709/224
6,807,156	B1 *	10/2004	Veres et al.	370/252
6,928,055	B2 *	8/2005	Ni	370/235
2003/0033403	A1 *	2/2003	Rhodes	709/224
2004/0136327	A1 *	7/2004	Sitaraman et al.	370/252

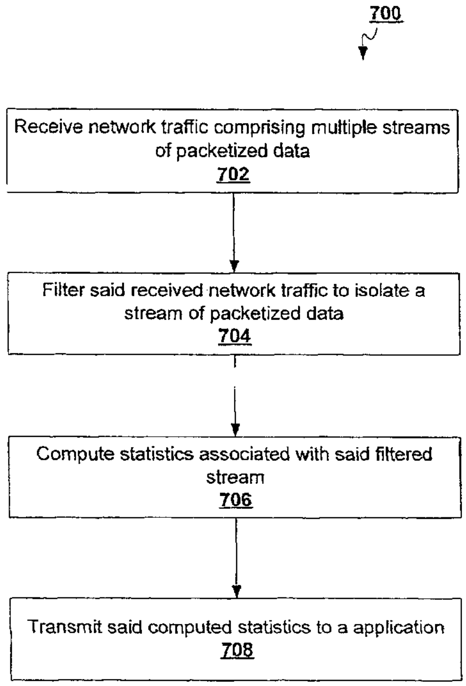
* cited by examiner

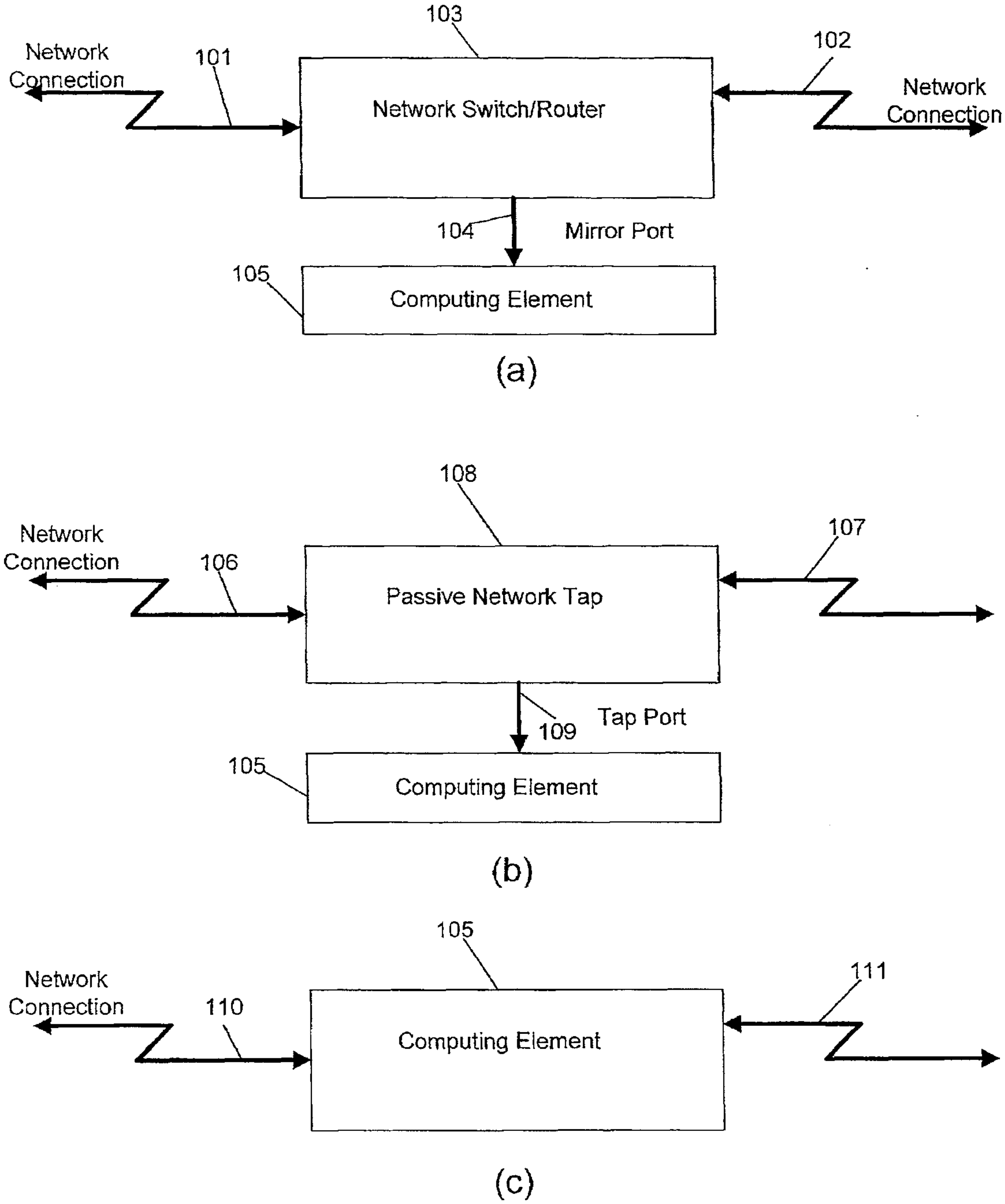
Primary Examiner—Ricky Q. Ngo
Assistant Examiner—Pao Sinkantarakorn
(74) *Attorney, Agent, or Firm*—IP Authority, LLC; Ramraj Soundararajan; William C. McBeth

(57) **ABSTRACT**

A packetized streaming media delivery network carries many "streams" of differing media content. They often are from multiple sources and of different media types. The invention consists of a scalable hardware and/or software computing element resolving the network traffic into its individual streams for focused, simultaneous, and continuous real-time monitoring and analysis. The monitoring and analysis consists of delay factor and media loss rate which measure the cumulative jitter of the streaming media within the delivery network and the condition of the media payload. These measurements form a powerful picture of network problem awareness and resolution. The delay factor objectively indicates the contribution of the network devices in the streams' path, allowing for both problem prediction and indication. In one example, tapping a packetized network at various locations allows for correlation of the same-stream performance at various network points to pinpoint the source(s) of the impairment(s).

28 Claims, 7 Drawing Sheets


700
Receive network traffic comprising multiple streams of packetized data
702
Filter said received network traffic to isolate a stream of packetized data
704
Compute statistics associated with said filtered stream
706
Transmit said computed statistics to a application
708


103
Network Connection
101
102
Network Switch/Router
Network Connection
104
Mirror Port
105
Computing Element
108
Network Connection
106
107
Passive Network Tap
109
Tap Port
105
Computing Element
105
Network Connection
110
111
Computing Element

(a)

(b)

(c)

Figure 1

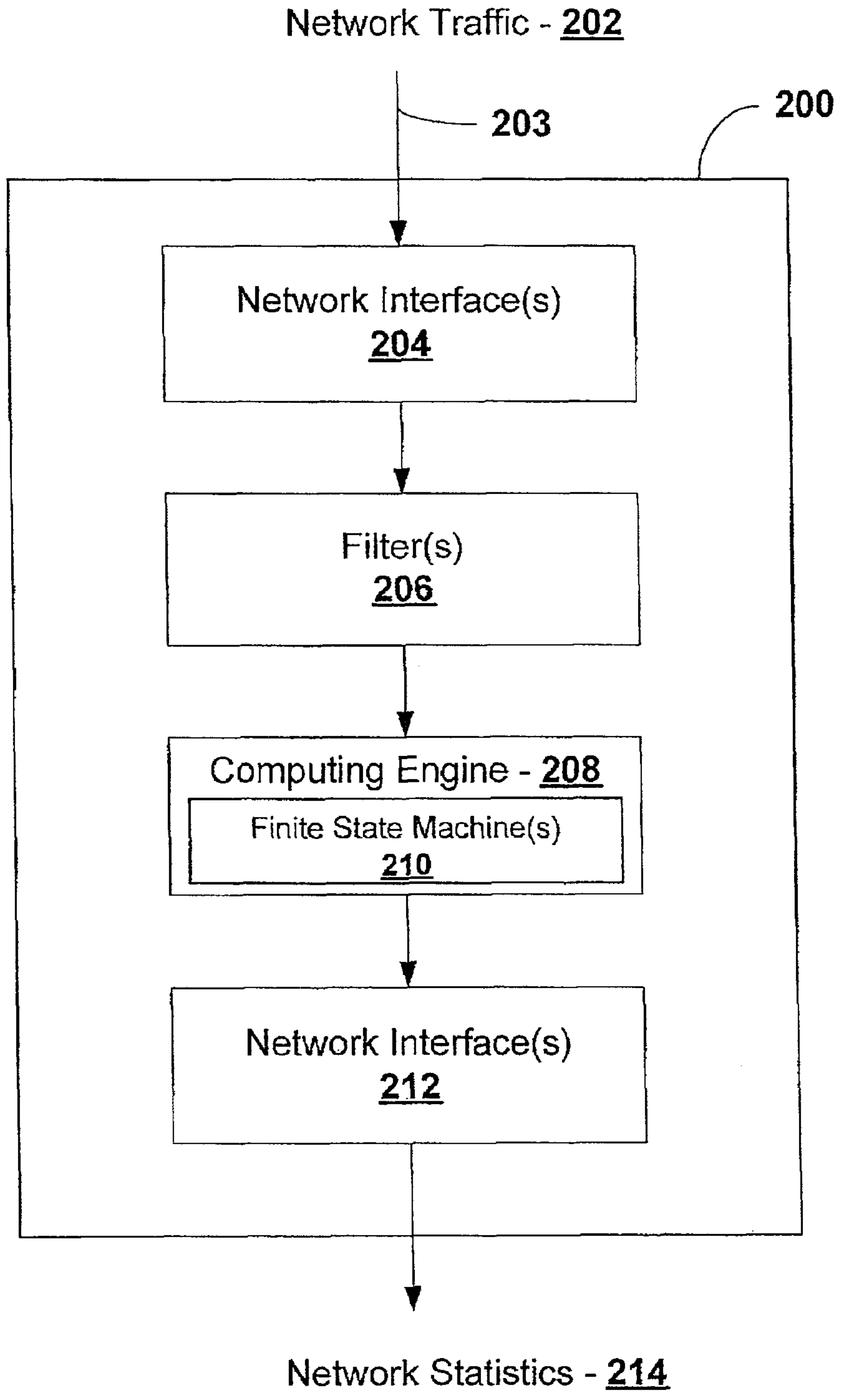

Network Traffic - 202
203
200
Network Interface(s) 204
Filter(s) 206
Computing Engine - 208
Finite State Machine(s) 210
Network Interface(s) 212
Network Statistics - 214

FIGURE 2

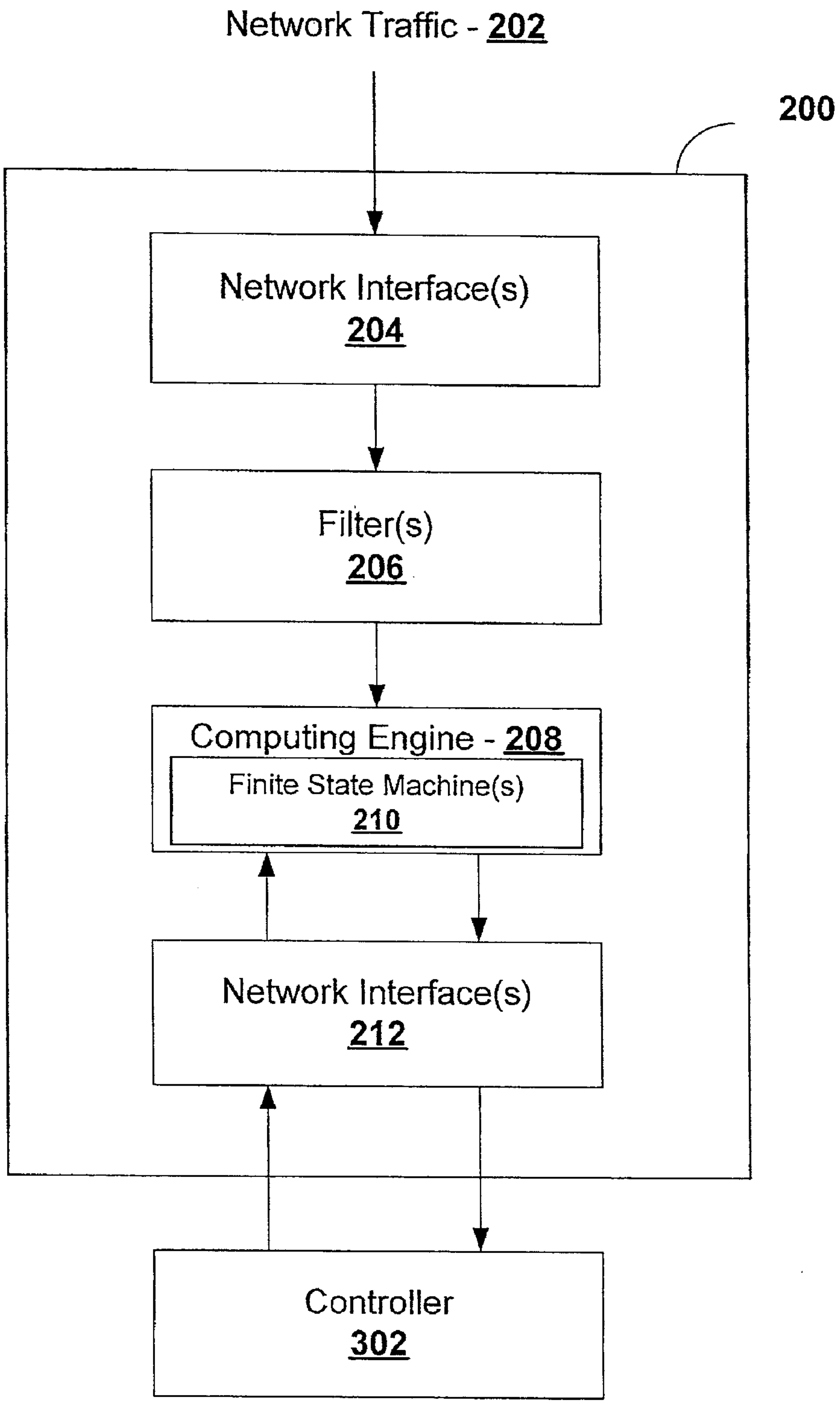

Network Traffic - 202
200
Network Interface(s)
204
Filter(s)
206
Computing Engine - 208
Finite State Machine(s)
210
Network Interface(s)
212
Controller
302

FIGURE 3

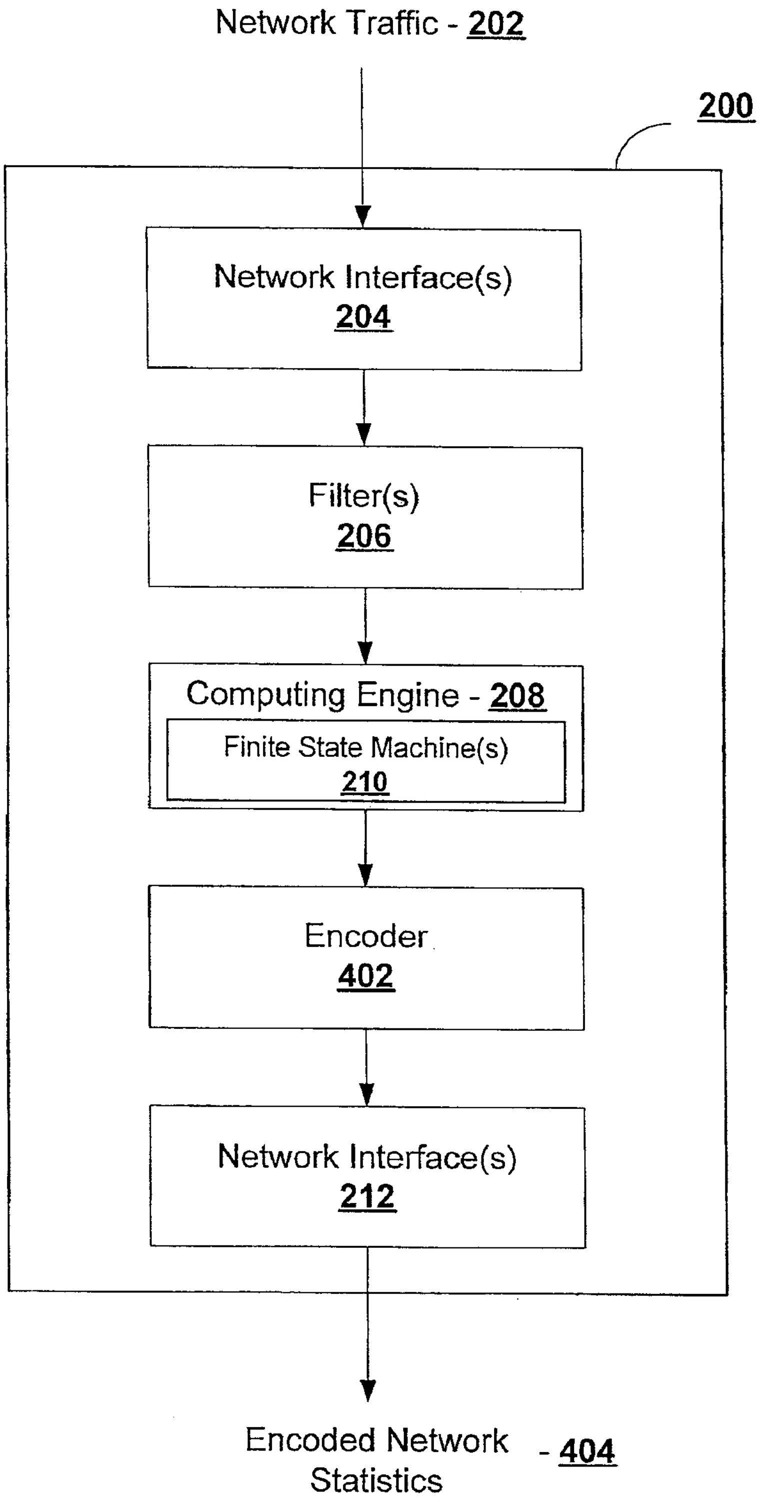

Network Traffic - 202
200
Network Interface(s)
204
Filter(s)
206
Computing Engine - 208
Finite State Machine(s)
210
Encoder
402
Network Interface(s)
212
Encoded Network Statistics - 404

FIGURE 4

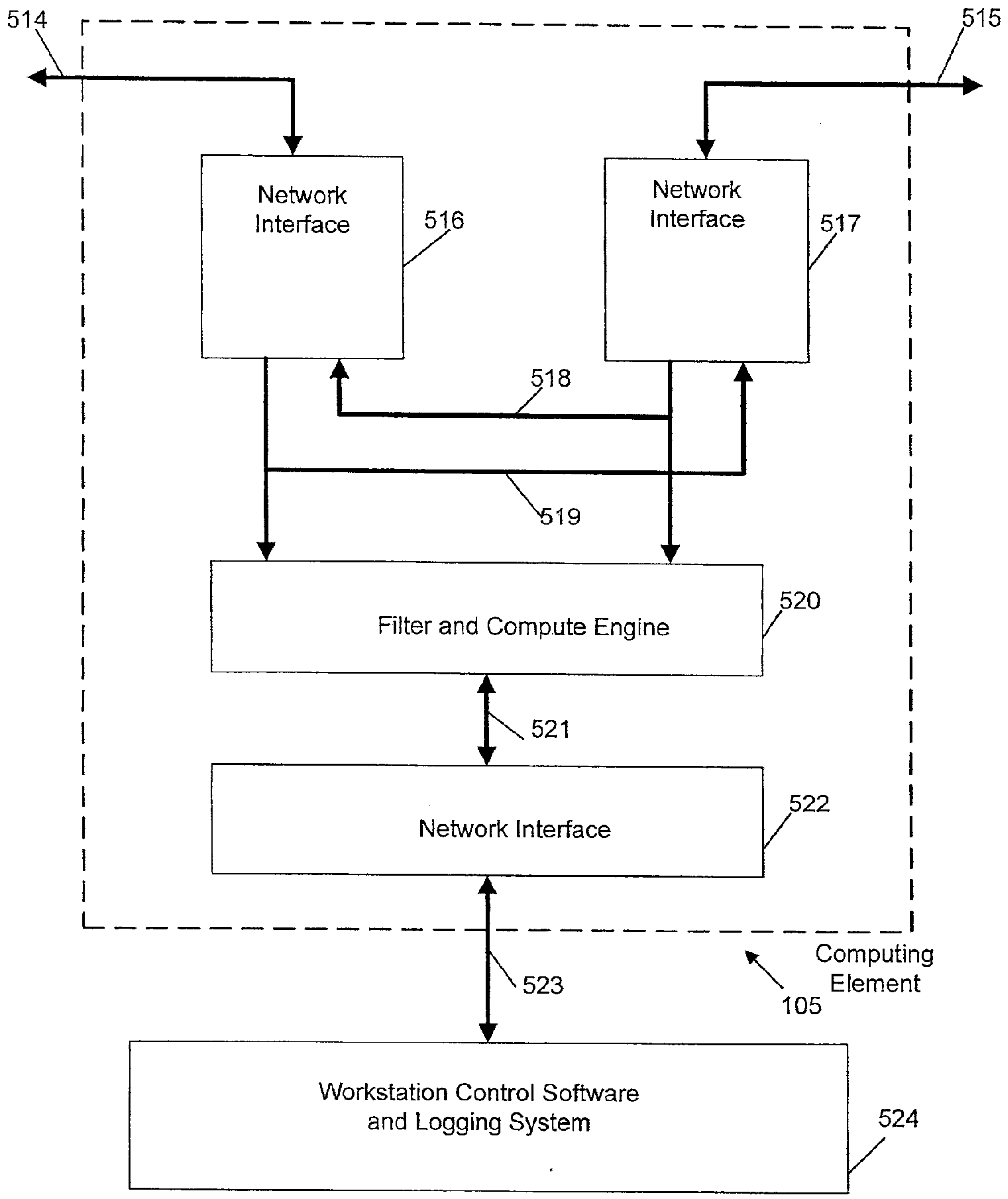

514
515
Network Interface
516
Network Interface
517
518
519
Filter and Compute Engine
520
521
Network Interface
522
523
Computing Element
105
Workstation Control Software and Logging System
524

Figure 5

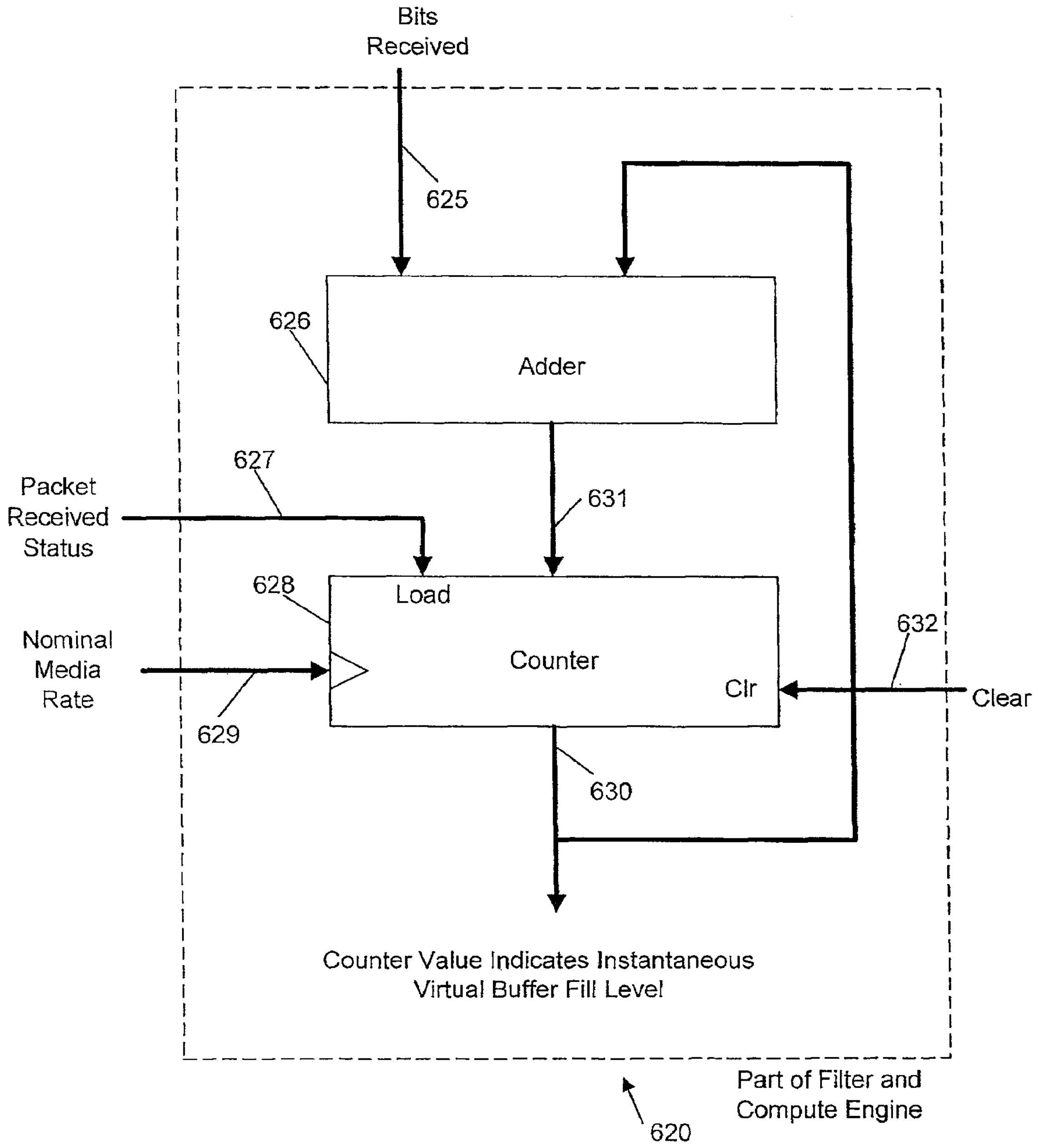

Bits
Received
625
626
Adder
627
631
Packet
Received
Status
628
Load
Nominal
Media
Rate
Counter
Clr
632
Clear
629
630
Counter Value Indicates Instantaneous
Virtual Buffer Fill Level
Part of Filter and
Compute Engine
620

Figure 6

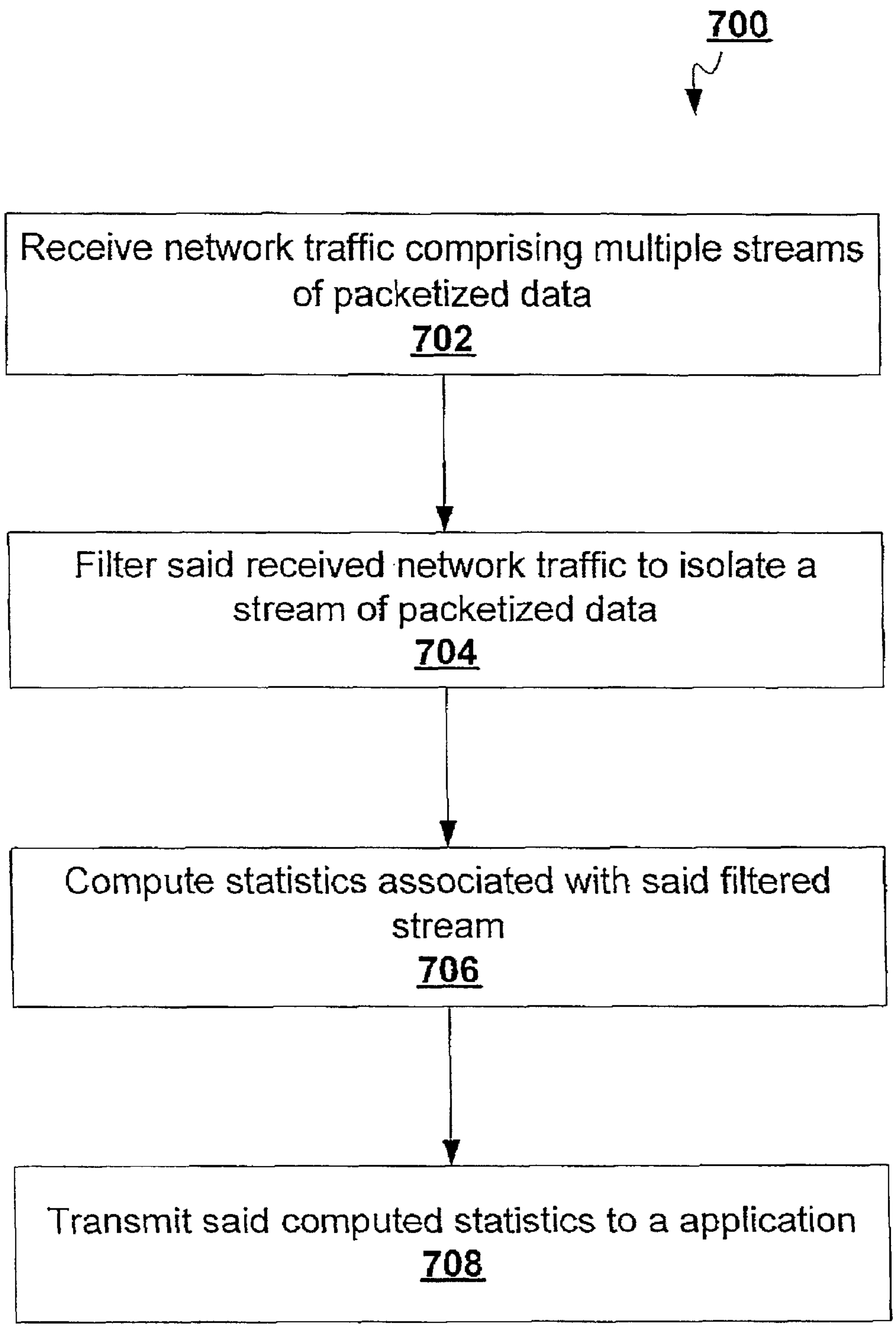

700
Receive network traffic comprising multiple streams of packetized data
702
Filter said received network traffic to isolate a stream of packetized data
704
Compute statistics associated with said filtered stream
706
Transmit said computed statistics to a application
708

FIGURE 7

SYSTEM AND METHOD FOR ANALYZING THE PERFORMANCE OF MULTIPLE TRANSPORTATION STREAMS OF STREAMING MEDIA IN PACKET-BASED NETWORKS

BACKGROUND OF INVENTION

1. Field of the Invention

The present invention relates generally to the field of streaming. More specifically, the present invention is related to analyzing streaming data in packetized form.

2. Discussion of Prior Art

Many electronic networks such as local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs) are increasingly being used to transport streaming media whose real-time data transport requirements exhibit high sensitivity to data loss and delivery time distortion. The technical literature is replete with various schemes to implement Quality of Service (QOS) on such networks to address the requirements of streaming media, especially when intermixed with conventional, time-insensitive, guaranteed delivery protocol stack data traffic. Furthermore, for efficiency reasons, the streaming media transport often uses a non-guaranteed delivery upper layer protocol stack such as UDP/IP making recovery of data in the presence of packet loss difficult. Regardless of whether QOS-enabled or non-QOS-enabled networks are employed, it is necessary to monitor the behavior of packet loss, delivery time distortion, and other real-time parameters of the network to assure satisfactory quality streaming media delivery.

There exists a variety of defined Management Information Bases (MIBs) which include definitions for a number of network parameters such as packet loss, inter-arrival times, errors, percentage of network utilization, etc., whose purpose is to indicate to a network manager the general operating conditions of the network. Such traditional forms of monitoring network behavior cannot easily indicate the effects that network performance has on a single or a group of individual streaming media streams. Data gathering from MIBs operating across a range of network layers combined with a highly skilled and experienced practitioner would be required to simply determine the jitter imposed on a single MPEG video stream, for instance, and would only be possible by post-processing data gathered while the network was in operation. Determining the cause of a fault in a streaming media stream may be possible through such analysis but lacks the real-time indication of a network fault that is required to maintain high-quality networks such as for video or audio delivery. It also does not address the need to monitor large numbers of streams in real-time such as streams of Video-on-Demand (VoD) networks using less technically skilled operations personnel, as would be necessary to enable implementation of continuous cost-effective quality control procedures for widely deployed networks such as for VoD.

Histograms are often used in prior art schemes to present the arrival time behavior of packets on a network, but such histograms only represent the aggregate behavior of packets arriving at the measurement node due to the need to combine MIB data from a range of network layers to extract sufficient information to track a particular stream's performance. Traditional histograms define the jitter between any two packets. Streaming media requires more in-depth knowledge, such as the time variation across many packets referred to as the "network jitter growth". This network jitter growth affects the streaming media quality as experienced by the user due to intermediate buffer overflow/underflow between the media source and its destination.

Network jitter growth of a media stream due to traffic congestion can also be an indicator of an impending fault condition and can thus be used to avoid transport failures rather than simply to react to faults after they occur. Conventional post-processed MIB analysis is inadequate for these purposes as described above.

The concept of regulating stream flow in a network based on the leaky bucket paradigm describes a methodology that might be used to prevent intermediate buffer overflow and packet jitter by regulating the outflow of data based on a set of parameters configured to optimize a particular flow. This does not address the need to analyze and continuously monitor multiple streams as is required during the installation and operation of networks carrying streaming media, especially for those enterprises whose revenue is derived from the high quality delivery of streaming media, such as broadcast and cable television entities.

A common prior art scheme used to effectively monitor multiple video streams is to decode each stream's MPEG content (for the video example) and display the streams on a large group of television screens. Monitoring personnel then watch the screens looking for any anomalous indications and take appropriate corrective action. This is a highly subjective and error prone process, as there is a possibility that a transient fault might be missed. This is also a reactive process, as corrective action can only be taken after a fault has occurred. Furthermore, this is also an expensive process in terms of both equipment and personnel costs. It also provides little or no indications of the root cause of the fault, thus adding to the time required for implementing corrective action. This approach also does not easily scale to modern video delivery systems based upon emerging, cost-effective high-bandwidth, networks intended to transport thousands of independent video streams simultaneously. In addition, this approach cannot pinpoint the location of the fault. To do so, the personnel and equipment must be replicated at multiple points in the distribution network, greatly increasing the cost. For this to be effective, the personnel must monitor the same stream at exactly the same time for comparison.

Many types of network delivery impairments are transient in nature affecting a limited number of packets during a period of momentary traffic congestion, for example. Such impairments or impairment patterns can be missed using traditional monitoring personnel watching video monitors. By not recognizing possible repeating impairment patterns, faults can exist for much longer periods because after the fault has passed, there is no residual trace information available for analysis. The longer a fault persists, the worse the customer satisfaction levels, and the greater the potential for lost revenues.

Whatever the precise merits, features, and advantages of the above-mentioned prior art schemes, they fail to achieve or fulfill the purposes of the present invention.

SUMMARY OF INVENTION

The present invention provides for a system and method for analyzing packetized network traffic. In one embodiment, the system comprises: (a) one or more interfaces to forward a copy of the network traffic comprising one or more streams; (b) one or more filters to receive and filter the forwarded network traffic to isolate at least one stream; and (c) a native streaming interface to receive packetized data corresponding to the isolated stream(s), wherein the native streaming interface provides minimum time distortion to permit media stream analysis and monitoring to indicate the network's influence on the isolated stream(s) and measure each isolated stream's conformance to a pre-determined stream standard.

In one embodiment, the system for analyzing packetized network traffic comprises: (a) a compute engine to compute statistics associated with an isolated stream, wherein the statistics for each stream comprise at least a delay factor (DF) defining an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth; and (b) one or more interfaces to forward the computed statistics for each streams of interest to a data consumer.

In another embodiment, the present invention provides for a system and method for analyzing packetized network traffic comprising one or more transportation streams. The system comprises: (a) one or more network interfaces to receive streaming network traffic associated with the transportation streams; (b) one or more filters to filter one or more streams of interest in the received transportation streams; (c) a compute engine comprising one or more finite state machines to compute index values associated with the streams of interest, wherein the index values for each stream comprising at least: a delay factor (DF) and a media loss rate (MLR); and (d) one or more interfaces to forward the computed index values for the streams of interest to a data consumer.

In another embodiment, the present invention's method comprises the steps of: (a) receiving network traffic comprising one or more transportation streams; (b) filtering the received traffic and isolating a transportation stream from the transportation streams; (c) computing statistics associated with the isolated transportation stream, wherein the statistics comprise at least a delay factor (DF) and a media loss rate (MLR); and (d) forwarding the computed statistics to a data consumer.

The DF value defines an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth, and the MLR value represents the number of media packets lost or corrupted.

BRIEF DESCRIPTION OF DRAWINGS

FIGS. **1***a-c* illustrate several methods of tapping an existing network traffic flow via the present invention's computing element.

FIG. **2** illustrates one embodiment of the present invention's computing element which analyzes network traffic.

FIG. **3** illustrates an extended embodiment of the present invention wherein a controller is used for controlling the computing element.

FIG. **4** illustrates another extended embodiment of the present invention wherein an encoder is used to encode the statistics calculated by the computing engine.

FIG. **5** illustrates an internal block diagram of the computing element and its interconnection with the control and logging system.

FIG. **6** illustrates an adder and a counter that form a part of the compute engine.

FIG. **7** illustrates a method associated with the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

While this invention is illustrated and described in a preferred embodiment, the invention may be produced in many different configurations. There is depicted in the drawings, and will herein be described in detail, a preferred embodiment of the invention, with the understanding that the present disclosure is to be considered as an exemplification of the principles of the invention and the associated functional specifications for its construction and is not intended to limit the invention to the embodiment illustrated. Those skilled in the art will envision many other possible variations within the scope of the present invention.

Many streaming media systems, such as VoD, broadcast television control centers, or satellite-based video distribution operations utilize packetized data networks for their low-cost and omnipresence in modern data systems. The present invention monitors these existing network conduits by sampling the data contained therein with minimal alteration of its characteristics.

FIGS. **1***a-c* illustrate several methods of tapping an existing network traffic flow via the present invention's computing element **105**. FIG. **1***a* illustrates a setup wherein an ordinary network switch or router **103**, which, while performing packet switching or routing on the traffic from its many ports, such as **101** and **102**, also provides for a "mirror" or "monitor" port **104**. Port **104** makes all data from a desired port available to the present invention's computing element **105**. Alternatively, as shown in FIG. **1***b*, a passive network tap **108** diverts a portion of the network traffic flow energy from one network port **106** to the other network port **107** and transmits that portion via a port **109** to the present invention's computing element **105**. FIG. **1***c* illustrates yet another method to tap the existing network flow via inserting the present invention's computing element **105** directly in-line with the network link to be observed via network ports **110** and **111**.

In the examples of FIGS. **1***a-b*, the computing elements **105** used in each case are identical. In the example of FIG. **1***c*, the computing element **105** also actively forwards all traffic from network connection **110** to network connection **111** and vice versa, while simultaneously providing all traffic to the equivalent internal functionality of the computing elements designated **105**.

FIG. **2** illustrates one embodiment of the present invention's computing element **105** which analyzes network traffic **202**. Computing element **105** comprises at least one network interface **204** to receive network traffic, one or more filters **206** to filter the received network traffic, at least one computing engine **208** to compute network statistics associated with the filtered network traffic via one or more finite state machines **210**, and at least one network interface **212** to accept control instructions and transmit the computed statistics to a data consumer. Network interface **204** interfaces with the network link to be monitored via network connections **203**. Network link protocols that support such packet-based transmission include, but are not limited to, 802.3 (Ethernet), 802.4, 802.5, USB, ATM, SONET, 802.11, Fibre-channel, Firewire or 1394, Infiniband, Bluetooth, 802.11, 802.15, 802.16, 802.17, ZigBee, or a native streaming video interface such as DVB-ASI.

The streaming media traffic of interest, which may consist of many individual streams of traffic, is filtered (via one or more filters **206**) from the incoming network traffic **202** and processed by the finite state machines **210** of computing engine **208** to reduce its measured transmission characteristics to a set of statistics or critical parameters known as an "Index". The Index can be communicated to a logging system with alarm values set for convenient human monitoring. For example, warnings can be forwarded to a data consumer when the computed statistics exceeds a predetermined threshold or rate-of-change. It should be noted that one computing engine can be used to track several streams of interest. Similarly, one or more computing engines can be used to track several streams of interest. Hence, the number of computing engines or the number of streams to be tracked should not be used to limit the scope of the present invention.

In one preferred embodiment, the Index, known as the Media Delivery Index (MDI) consists of two parts: the Delay Factor (DF) and the Media Loss Rate (MLR). This embodiment is especially valuable for constant bit rate MPEG-2 Transport Streams carried over a network such as a packetized network. The DF represents the Instantaneous Flow Rate Balance (IFRB) and is derived in the computing element. The MLR represents the number of lost or corrupted media packets and is readily derived from tracking the Continuity Counter (CC) for the MPEG-2 transport stream application or from a sequence counter or the like for protocols, such as RTP, which support the same. The MDI (DF:MLR) then represents the two key factors which describe the dynamic behavior of streaming media over packetized networks: packet jitter growth and packet loss. This Index provides at-a-glance determination of traffic impairment as well as an indication of the operating margin of a network. By modifying the calculation of the IFRB, the DF may also be used with variable bit rate streaming media transport over packetized networks.

FIG. **3** illustrates an extended embodiment of the present invention wherein a controller **302** is used for controlling the computing element **105**. Controller **302** transmits, via an interface, control instructions from a management system to modify system-level state-based logic data associated with the computing element **105**, and receives, via the interface, the analysis results generated by the computing element **105**.

FIG. **4** illustrates another extended embodiment of the present invention wherein encoder **402** is used to encode the statistics calculated by computing engine **208**. Then, the encoded statistics **404** is transmitted to a data consumer via one or more interfaces **212**. Some examples of encoding include (but are not limited to) encryption (such as for security), compression, or code format conversion (e.g., convert data in an ASCII format for readability).

It should be noted that more than one network interface can be used to receive network traffic. For example, FIG. **5** illustrates computing element **105** (as used in FIG. **1***c*) with two network interfaces **516** and **517**, wherein computing element **105** is used for analyzing one or more streaming media flows. The two network interfaces **516** and **517** interface with the network link to be monitored via network connections **514** and **515**. As in FIG. **2**, network link protocols that support such packet-based transmission include, but are not limited to, 802.3 (Ethernet), 802.4, 802.5, USB, ATM, SONET, 802.11, Fibrechannel, Firewire or 1394, Infiniband, Bluetooth, 802.11, 802.15, 802.16, 802.17, ZigBee, or DVB-ASI. In operation, data received from network connection **515** is decoded via network interface **517** and the resulting data is forwarded to the filter and compute engine **520** and to the other network interface **516**. Then, network interface **516** forwards the data to the network connection **514**, thus completing the connection from network interface **515**. Thus, all data received from network interface **515** is forwarded to network interface **514** with a

minimum of distortion while making all the same data available for analysis by other components of the computing element. Likewise, all data from network connection **514** is forwarded to network connection **515** while also being forwarded to the filter and compute engine **520**. The result is a continuous full duplex connection between network connections **514** and **515** providing an uninterrupted network traffic flow while simultaneously providing all network data to the filter and compute engine **520**. Alternatively, as per FIG. **1***a* and FIG. **1***b*, the computing element **105** may require only a single network interface, but otherwise performs as described above, with network data being forwarded to the filter and compute engine **520**.

The filter and compute engine **520** is configured via interface **521** such that it can filter the desired streaming media flows from other network traffic types for further analysis. For example, to analyze MPEG-2 streaming video over UDP/IP protocols, the filter can be configured to accept only layer-2 packets with the IP protocol type and only IP frames with UDP protocol types and only UDP datagrams that encapsulate MPEG-2 transport streams. After performing the appropriate filtering function, the compute engine calculates the components that comprise the Index value for a given streaming media flow. The Index values, and other statistics regarding the flow, are forwarded to the network interface **522** via interface **521**. Then, interface **523** is used to convey the Index values to a data consumer such as an application running, for example, in a workstation consisting of control software and a logging system **524**, collectively referred to as a "management" system. Network Interface **522** need not be the same type as **516** or **517** (i.e., a RS-232 serial port). Its bandwidth via the choice of physical and link layer protocols may be scaled or sized to match the amount of data expected to be handled. It should be noted that network interface **522**, interface **523**, and workstation (management system) **524** may be physically co-located with the computing element **105** and need not be external.

In one embodiment, the compute engine comprises at least one finite state machine counter as shown in FIG. **6**. The finite state machine counter is used to compute an Instantaneous Flow Rate Balance (IFRB). Counter **628** is loaded when a packet has been received via **627**. The counter is loaded with the sum of the current count and the number of bits received in this packet **625** from the adder **626**. Counter **628** decrements its count at each clock input pulse **629** whose rate is set to the nominal streaming media rate. Further, counter **628** is cleared at any time via the **632** clear signal. The counter output **630** indicates the number of bits that have been received at the point of test but not yet consumed, assuming that a virtual terminal device which consumes or "uses" the streaming media flow (such as a video decoder for a streaming video media case) drains the data received at a nominal media rate at this network location. Thus, the counter output **630** represents the size of a buffer that would be needed to prevent data loss and absorb the network jitter growth due to data arriving via a packetized network. It should be noted that counter **628** may also result in negative numbers during periods between a burst of data thus representing the size of a virtual terminal's buffer needed to be prefilled to avoid underflow. Adder **626** and counter **628** may also be combined into a single entity to simply track the net difference between bits received on the packetized network side and the bits out based upon an expected drain rate. The actual quantity being tracked may be bits or any derivative thereof (bytes, words, etc.). It is important to note that the bits counted are only those subject to the drain rate. Typically, this is the payload of the packet (i.e., no headers or overhead.) For example, in the case of an MPEG-2 transport stream sent via Ethernet IP/UDP, the bits tracked would typically be the MPEG-2 transport stream packets contained within the Ethernet frame, excluding the IP/UDP headers and Ethernet CRC. The present invention further extends to using streaming media streams that are variable bit rate in nature. Variations in media bit rate may be accommodated by monitoring and updating the expected drain rate used in IFRB calculation along with the stream. Since this finite state machine is simple, it can operate at common media rate speeds and can be replicated easily and compactly if implemented in hardware such as an FPGA, ASIC, or discrete logic, making possible an array of such machines such that one may be dedicated to each streaming media flow. Furthermore, the filter and compute engine can also be configured to capture and track other streaming media flow parameters of interest such as an MPEG-2 transport steam's continuity counters to detect dropped or corrupted packets, stream identifiers, etc.

It should be noted that computing the Instantaneous Flow Rate Balance (IFRB), and thus DF, requires knowledge of the expected media drain rate either by prior knowledge or by measurement. The expected drain rate, and thus stream bitrate, may also be referred to as the media consumption rate, as this is the rate at which the receiver of the media stream must consume that stream. It is possible that the local estimation of the drain rate may drift or be offset with respect to the actual media streams' bitrate due to frequency drift or offset between the source of the media streams' clock and our local processing clock. This drift or offset causes monotonically increasing or decreasing IFRB and virtual buffer calculations, and may be mitigated by periodically clearing the current state of the IFRB and virtual buffer. Another approach utilizes a well known method entailing Phase Locked Loops (PLL) or Delay Locked Loops (DLL) to remove the drift or offset.

Returning to the discussion of FIG. **5**, streaming media flow parameters as described above can be forwarded via a network Interface **521**, and network connection **522**, and external network **523**, or via any type data interface as they are captured or buffered in a memory in the filter and compute engine for later retrieval by a workstation **524**. In some instances, the streaming media content itself may be presented to the workstation **524** via the same path for additional analysis. They may be combined with a time stamp at either the filter and compute engine **520** or the workstation **524**. Long term logs may be maintained by **524** for trend analysis, coincident analysis with other network events, the start and end of particular streaming media flows, etc. Alternatively, workstation **524** can show an instantaneous view of streaming media parameters for human monitoring. High and low watermark values may be set in the computing element **105** or in the workstation **524** for the Index parameter or any measured parameter, such that if exceeded, will be logged or trigger an alarm; this functionality may be used to warn of possible impending faults such as deviations from nominal in the flow rates that could cause a network or terminal device buffer to overflow or underflow. The Index value indicates the network's instantaneous operating jitter margin. Additionally, the rate of sampling of such parameters can be reduced to decrease the load on interface **523** during benign network conditions or increased to provide a more detailed analysis of an identified fault. Either the computing element or workstation **524** may produce long term analysis as well by performing additional computational operation on the IFRB.

In some instances, workstation **524** functionality may be integrated with the filter and compute engine for a direct display of information to the user.

It should be noted that a pure hardware, a pure software, and a hybrid hardware/software implementation of the filter and compute engine components is envisioned and should not be used to limit the scope of the present invention.

It should be noted that various kinds of interfaces can be used for establishing a packet-based communication session between the external interfaces (**514** or **515** or **523**) and the computing element, such as (but not limited to) a gigabit Ethernet network controller or a 10/100 Mbit/s Ethernet network interface card. Moreover, one skilled in the art can envision using various current and future interfaces and, hence, the type of packetized network interface used should not be used to limit the scope for the present invention.

In one embodiment, bandwidth for the transportation of network parameters via interface **523** as discussed above is allocated in an "on-demand" fashion, wherein full channel (network conduit) bandwidth is allocated and available to the data consumer. Compute engine **520** can track nearly any set of parameters or events, such as the last N-packets received or statistics acquired, storing it in a circular buffer. Thus, when a critical event occurs such as streaming media data loss, bandwidth would be allocated "on-demand" to report the tracking information leading up to the critical event to the workstation analysis device **524** through the interface **523**. Having pertinent information about what traffic the network was handling (not only at the time of the critical event but leading up to it as well) presented "on-demand" at the time of the critical event is very powerful. Having this information greatly reduces the "hunting" time required to identify the cause of the critical event. This information could be gathered remotely as well, given a suitable network type for **523**. Expanding on the "on-demand" possibilities for parameter reporting, bandwidth may also be allocated "on-demand" on either network interfaces **514** or **515** in an in-band reporting fashion, facilitating the monitoring by equipment on the same distribution network as the streaming media.

If the network Interface **523** is an ASI (Asynchronous Serial Interface, as in DVB-ASI) type and the streaming media content itself is presented to the Interface in such a way as to minimize instrument timing distortions, a conventional streaming media specific analyzer or monitor may be utilized to not only measure the stream's conformance to expected stream standards but also to indicate the influence of network behavior. In this configuration, the computing element may be thought of as a protocol converter as well.

The present invention's system can be used in debugging various embedded systems within the streaming media's transport network. Various equipment utilized in the transportation or creation of the streaming media may allow debugging and/or parameter manipulation via the transport network as well as provide its own statistical operational information (i.e., its own system "health"). This makes possible the cross-correlation of the system's overall state/health. The invention acquires such control information via a network channel and may use its filter and compute engine capabilities to provide either the raw or processed data to a Workstation Monitor/Logger as described for Index data above.

The present invention allows the implementer the ability to scale the amount of in-band or out-of-band measured or sampled data to pass through the system up to the maximum supported by the network conduit and down to nothing. Additionally, the present invention provides the ability to scale with improvements in network conduit technology. For example, the faster the network conduit, the more measurements or sampled data can pass. Moreover, as high-speed systems continue to evolve, their network conduit's bandwidth is usually increased proportionately to facilitate the use of the high-speed system itself (i.e., a faster network conduit is part of the main feature-set of the system; bandwidth is thereby increased by necessity). The present invention accommodates such increases in bandwidth associated with the network conduit and utilizes such high-speed systems to extract measurements or sampled data at a faster rate.

FIG. **7** illustrates a method **700** associated with an embodiment of the present invention. In step **702**, network traffic is received by a network interface, wherein the traffic comprises one or more streams of packetized data. Next, in step **704**, the received traffic is filtered to isolate at least one stream of packetized data. In step **706**, an Index is computed for the filtered stream of packetized data. In one preferred embodiment, the Index, known as the Media Delivery Index (MDI), consists of two parts: the Delay Factor (DF) and the Media Loss Rate (MLR). The DF represents the Instantaneous Flow Rate Balance (IFRB) and is derived in the computing element as described earlier. The MLR represents the number of lost or corrupted media packets and is readily derived from tracking the Continuity Counter (CC) for the MPEG-2 transport stream application or from a sequence counter or the like for protocols, such as RTP, which support the same. The MDI (DF:MLR) then represents the two key factors which describe the dynamic behavior of streaming media over packetized networks: packet jitter growth and packet loss. This Index provides at-a-glance determination of traffic impairment as well as an indication of the operating margin of a network. Then, in step **708**, the computed statistics are forwarded to a data consumer, such as one running in a workstation. In one embodiment, a quality of service (QOS) metering scheme is implemented based upon adjusting traffic priority between the forwarded computed network statistics and the streaming network traffic.

Furthermore, the present invention includes a computer program code-based product, which is a storage medium having program code stored therein which can be used to instruct a computer to perform any of the methods associated with the present invention. The computer storage medium includes any of, but not limited to, the following: CD-ROM, DVD, magnetic tape, optical disc, hard drive, floppy disk, ferroelectric memory, flash memory, ferromagnetic memory, optical storage, charge coupled devices, magnetic or optical cards, smart cards, EEPROM, EPROM, RAM, ROM, DRAM, SRAM, SDRAM, and/or any other appropriate static or dynamic memory or data storage devices.

Implemented in computer program code-based products are: (a) receiving network traffic comprising one or more transportation streams; (b) filtering the received traffic and isolating a transportation stream from the transportation streams; (c) computing statistics associated with the isolated transportation stream comprising at least a delay factor (DF) and a media loss rate (MLR), wherein DF defines an instantaneous flow rate balance representing a buffer size that is needed to prevent data loss and absorb network jitter growth, and MLR represents the number of media packets lost or corrupted; and (d) forwarding the computed statistics to a data consumer.

CONCLUSION

A system and method has been shown in the above embodiments for the effective implementation of a system and method for measuring and exposing the dynamic behavior of streaming media over a packet-based network. While various preferred embodiments have been shown and described, it will be understood that there is no intent to limit the invention by such disclosure but, rather, it is intended to cover all modifications and alternate constructions falling within the spirit and scope of the invention as defined in the appended claims. For example, the present invention should not be limited by the number of network interfaces, number of filters, number of streams handled by the compute engine, type of packetized network conduit, location of control software, choice of hardware or software implementation of bandwidth provisioning or filter or compute engine, type of streaming media data, choice of hardware or software implementation of the "on-demand" embodiment, computing environment, or specific hardware associated with the network interfaces, filter device, or compute engine system.

The above systems are implemented in various computing environments. For example, the present invention may be implemented on a conventional IBM PC or equivalent, multi-nodal system (e.g., LAN) or networking system (e.g., Internet, WWW, wireless web). All programming and data related thereto are stored in computer memory, static or dynamic or non-volatile, and may be retrieved by the user in any of: conventional computer storage, display (i.e., CRT) and/or hardcopy (i.e., printed) formats. The programming of the present invention may be implemented by one skilled in the art of computer systems and/or software design.

The invention claimed is:

1. A method for analyzing packetized network traffic comprising the steps of:

a. receiving a copy of said network traffic comprising one or more streams;

b. filtering said received network traffic to isolate each stream from said one or more streams;

c. forwarding packetized data corresponding to each stream to a native streaming interface, said native streaming interface providing minimum time distortion as compared to said network traffic to permit media stream analysis and monitoring to indicate said network's influence on each isolated stream and measure each isolated stream's conformance to a pre-determined stream standard;

d. computing statistics associated with each isolated stream, said statistics comprising at least a delay factor (DF) parameter defining an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth; and

e. forwarding, for each isolated stream, said computed statistics to a data consumer.

2. The method for analyzing packetized network traffic, as per claim **1**, wherein said computed statistics additionally comprises a media loss rate (MLR) parameter representing number of media packets lost or corrupted.

3. A system for analyzing packetized network traffic comprising:

a. one or more interfaces to forward a copy of said network traffic comprising one or more streams;

b. one or more filters to receive and filter said forwarded network traffic to isolate each stream from said one or more streams;

c. a native streaming interface to receive packetized data corresponding to each isolated stream, said native streaming interface providing minimum time distortion by determining an arrival time of a given packet to be as close to when it is received by said interface in (a) to permit media stream analysis and monitoring to indicate said network's influence on said each isolated stream and measure each isolated stream's conformance to a pre-determined stream standard;

d. a compute engine to compute statistics associated with said at least one isolated stream, said statistics for each stream comprising at least a delay factor (DF) defining an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth; and

e. one or more interfaces to forward said computed statistics for said one or more streams of interest to a data consumer.

4. The system for analyzing packetized network traffic, as per claim **3**, wherein said computed statistics additionally comprise a media loss rate (MLR) parameter, said MLR representing number of media packets lost or corrupted.

5. A method for analyzing packetized network traffic comprising one or more streams, said method comprising the steps of:

a. receiving said network traffic comprising one or more streams;

b. filtering said received network traffic and isolating at least one stream from said one or more streams;

c. computing statistics associated with each isolated stream, said statistics comprising at least a delay factor (DF) parameter defining an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth; and

d. forwarding for each isolated stream, said computed statistics to a data consumer.

6. The method for analyzing packetized network traffic comprising one or more streams, as per claim **5**, wherein said computed statistics additionally comprise a media loss rate (MLR) parameter representing number of media packets lost or corrupted.

7. The method for analyzing packetized network traffic comprising one or more streams, as per claim **5**, wherein said method further comprises the step of recovering control information associated with said one or more streams and forwarding said recovered control information to said data consumer.

8. The method for analyzing packetized network traffic comprising one or more streams, as per claim **5**, wherein bandwidth for forwarding said computed statistics to a data consumer is allotted in an on-demand manner by increasing said bandwidth usage when computed statistics indicate a warning.

9. The method for analyzing packetized network traffic comprising one or more streams, as per claim **5**, wherein said computed statistics additionally comprise any of the following: stream instantaneous bit-rate, average bit-rate, deviation from nominal bit-rate, minimum and maximum deviation from nominal bit-rate, instantaneous flow rate deviation, or minimum and maximum instantaneous flow rate deviation.

10. The method for analyzing packetized network traffic comprising one or more streams, as per claim **8**, wherein the number of said computed statistics or a rate at which said statistics are computed is reduced during benign network conditions and increased for detailed analysis of each of said isolated streams.

11. The method for analyzing packetized network traffic comprising one or more streams, as per claim **5**, wherein said instantaneous flow rate balance value is computed from said each isolated stream via a counter computing an instantaneous flow rate and said counter registers a deviation from nominal as an indication of the flow's instantaneous accumulated jitter for forwarding to said data consumer.

12. The method for analyzing packetized network traffic comprising one or more streams, as per claim **11**, wherein said instantaneous flow rate balance value is periodically cleared to avoid monotonically increasing values due to differences in calculated bit rate values caused by offset or drift in frequency in a local clock source.

13. The method for analyzing packetized network traffic comprising one or more streams, as per claim **5**, wherein said method further comprises the step of implementing a quality of service (QOS) metering scheme based upon adjusting traffic priority between said forwarded computed network statistics and said streaming network traffic.

14. An article of manufacture comprising computer usable medium encoded with computer executable instructions embodied therein which analyzes packetized network traffic comprising one or more streams, said medium comprising:

a. computer executable instructionsaiding in receiving said network traffic comprising one or more streams;

b. computer executable instructions filtering said received traffic and isolating at least one stream from said one or more streams;

c. computer executable instructions computing statistics associated with each isolated stream, said statistics comprising at least a delay factor (DF) parameter defining an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth; and

d. computer executable instructions aiding in forwarding said computed statistics to a data consumer.

15. The article of manufacture comprising computer usable medium encoded with computer executable instructions embodied therein which analyzes packetized network traffic comprise one or more streams, as per claim **14**, wherein said computed statistics additionally comprises a media loss rate (MLR) parameter representing number of media packets lost or corrupted.

16. The article of manufacture comprising computer usable medium encoded with computer executable instructions embodied therein which analyzes packetized network traffic comprising one or more streams, as per claim **14**, wherein said medium further comprises computer executable instructions encoding said computed statistics prior to forwarding.

17. A system analyzing packetized network traffic comprising one or more streams, said system comprising:

a. one or more network interfaces to receive streaming network traffic associated with said one or more streams;

b. a filter and compute engine to filter one or more streams of interest in said one or more streams and compute statistics associated with said one or more streams of interest, said statistics for each stream comprising at least a delay factor (DF) defining an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth for said stream; and

c. one or more interfaces to forward said computed statistics for said one or more streams of interest to a data consumer.

18. The system analyzing packetized network traffic comprising one or more streams, as per claim **17**, wherein said computed statistics additionally comprise a media loss rate (MLR) parameter representing number of media packets lost or corrupted.

19. The system analyzing packetized network traffic comprising one or more streams, as per claim **17**, wherein said instantaneous flow rate balance value is computed from said one or more streams of interest via a counter computing an instantaneous flow rate and said counter registers a deviation from nominal as an indication of the flow's instantaneous accumulated jitter for forwarding to said data consumer.

20. The system analyzing packetized network traffic comprising one or more streams, as per claim **17**, wherein said instantaneous flow rate balance value is periodically cleared to avoid monotonically increasing values due to differences in calculated bit rate values caused by offset or drift in frequency in a local clock source.

21. The system analyzing packetized network traffic comprising one or more streams, as per claim **17**, wherein said one or more interfaces forward said computed statistics to a data consumer in an in-band manner by sharing network transmission bandwidth between said streaming network traffic and computed statistics.

22. The system analyzing packetized network traffic comprising one or more streams, as per claim **17**, wherein a quality-of-service (QOS) metering scheme is implemented based upon adjusting traffic priority between said computed statistics and said streaming network traffic.

23. The system analyzing packetized network traffic comprising one or more streams, as per claim **17**, wherein frequency of said computed statistics to be forwarded is scaled linearly with bandwidth associated with said one or more interfaces used to forward said computed statistics.

24. The system analyzing packetized network traffic comprising one or more streams, as per claim **17**, wherein at least one of said interfaces is a native streaming video interface forwarding a streaming media payload, said native streaming video interface providing minimum time distortion to permit media stream analysis and monitoring by a native streaming media analyzer.

25. A system analyzing packetized network traffic comprising one or more streams, said system comprising:

a. one or more network interfaces to receive streaming network traffic associated with said one or more streams;

b. one or more filters to filter one or more streams of interest in said one or more streams;

c. a compute engine comprising one or more finite state machines to compute index values associated with said one or more streams of interest said index values for each stream comprising at least a delay factor (DF) and a media loss rate (MLR), said DF defining an instantaneous flow rate balance representing a virtual buffer delay that is needed to prevent data loss and absorb network jitter growth for said stream, and said MLR representing number of media packets lost or corrupted for said stream; and

d. one or more interfaces to forward said computed index values for said one or more streams of interest to a data consumer.

26. The system analyzing packetized network traffic comprising one or more streams, as per claim **25**, wherein a quality-of-service (QOS) metering scheme is implemented based upon adjusting traffic priority between said computed index values and said streaming network traffic.

27. The system analyzing packetized network traffic comprising one or more streams, as per claim **25**, wherein frequency of said computed index values to be forwarded is scaled linearly with bandwidth associated with said one or more interfaces used to forward said computed index values.

28. The system analyzing packetized network traffic comprising one or more streams, as per claim **25**, wherein at least one of said interfaces is a native streaming video interface forwarding a streaming media payload, said native streaming video interface providing minimum time distortion to permit media stream analysis and monitoring by a native streaming media analyzer.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,321,565 B2
APPLICATION NO. : 10/604997
DATED : January 22, 2008
INVENTOR(S) : Marc Todd et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 12, Line 27, delete "instructionsaiding" and insert --instructions aiding--.

Signed and Sealed this

Sixth Day of May, 2008

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office